Oslo

Kommunerevisjonen

2023

Personvern i skoler

Hauketo skole
Nordseter skole

Rapport 2

Kommunerevisjonen – integritet og verdiskaping

Siste publikasjoner fra Kommunerevisjonen i Oslo

Kommunerevisjonens rapporter 2023

Rapport 1/2023	Eierskapskontroll av Oslo Business Region AS

Kommunerevisjonens rapporter 2022

Rapport 1/2022	Fossil- og utslippsfrie bygge- og anleggsplasser
Rapport 2/2022	Oppsummering av utvalgte undersøkelser gjennomført i regnskapsrevisjonen 2021
Rapport 3/2022	Sykkelsatsingen i Oslo
Rapport 4/2022	Bemanning i barnehager
Rapport 5/2022	Plan- og bygningsetatens arbeid med ulovlighetsoppfølging
Rapport 6/2022	Oppfølging etter rapport 6/2019 Vg3 fagopplæring i skole
Rapport 7/2022	Kostnadsoverskridelser i store og unike investeringsprosjekter
Rapport 8/2022	Eierskapskontroll - Oppfølgingen av Oslomodellen og samfunnsansvar
Rapport 9/2022	Eierskapskontroll av Fjellinjen AS
Rapport 10/2022	Økonomisk stønad til store barnefamilier
Rapport 11/2022	Oppfølging etter rapport 8/2019: Bemanning og kontinuitet i hjemmetjenesten
Rapport 12/2022	Ansettelser av ledere
Rapport 13/2022	Planlegging av anskaffelser
Rapport 14/2022	Arbeidsforberedende trening Oslo Produksjon og Tjenester Spir Arbeidsinkludering
Rapport 15/2022	Beredskap ved bortfall av vann

Du finner mer informasjon om Kommunerevisjonen og våre rapporter på
www.krv.oslo.kommune.no

Forord

Denne rapporten er et resultat av forvaltningsrevisjonen av personvern i skoler.

Undersøkelsen er forankret i kontrollutvalgets vedtak av 31. august 2021 (sak 58) og tilhører området virksomhetsstyring, digitalisering og informasjonssikkerhet, jf. bystyrets vedtak om *Overordnet analyse og plan for forvaltningsrevisjon* og eierskapskontroll 2020–2024 av 21. oktober 2020 (sak 283).

Forvaltningsrevisjon er en lovpålagt oppgave for Oslo kommune. Forvaltningsrevisjon er definert slik i kommuneloven § 23-3:

> Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak.

Forvaltningsrevisjon i Oslo kommune gjennomføres iht. gjeldende standard for forvaltningsrevisjon i kommuner og fylkeskommuner i Norge (RSK 001).

Prosjektet er gjennomført av seniorrådgiverne Stig Eliassen og Siri Strandenæs Lode, med sistnevnte som prosjektleder.

Vi vil takke Byrådsavdeling for oppvekst og kunnskap, Utdanningsetatens administrasjon, Hauketo skole, Nordseter skole og elevrådsrepresentanter for nødvendig bistand i løpet av prosjektet.

18.01.2023

Hilde Ludt
avdelingsdirektør

Siri Strandenæs Lode
seniorrådgiver

Innhold

Hovedbudskap

Kommunerevisjonen har undersøkt om personopplysninger om elever er tilstrekkelig sikret på Hauketo skole og Nordseter skole.

Det var iverksatt tiltak i Utdanningsetaten sentralt og på de to skolene for å bidra til en tilfredsstillende behandling av elevers personopplysninger.

Behandlingen av elevers personopplysninger var likevel ikke tilfredsstillende. Utdanningsetaten hadde ikke ferdigstilt personvernkonsekvensvurderinger for læringsteknologien som var i bruk i Osloskolen, og det var svakheter og mangler ved skolenes kartlegging, risikovurdering og avvikshåndtering. Ikke alle tilganger til sensitive personopplysninger var i tråd med tjenstlig behov, og skolene manglet et verktøy for samhandling mellom ledelse og lærere for behandling av særlige kategorier personopplysninger.

Sammendrag

Alle skoler behandler en mengde personopplysninger om elevene. Dette omfatter for eksempel opplysninger om fravær, anmerkninger, familieforhold, helse, eventuelle lærevansker mv. Utdanningsetaten har også ansvar for mange systemer med et stort antall brukere, både læringsteknologiske systemer og administrative systemer. Dersom Utdanningsetaten og skolene ikke har tilfredsstillende rutiner og praksis for håndtering av personopplysninger, kan det blant annet medføre at informasjon kommer på avveie eller går tapt.

Kommunerevisjonen har undersøkt om personopplysninger om elevene er tilstrekkelig sikret i skoler i Oslo.

For å besvare problemstillingen har vi undersøkt følgende temaer:
- kartlegging av informasjonsverdier og risikovurdering og -håndtering
- tilgangsstyring
- opplæring og kompetanse
- avvikshåndtering

Revisjonskriteriene er målestokken som Kommunerevisjonen legger til grunn for sine vurderinger. De viktigste kildene til revisjonskriterier i undersøkelsen har vært personopplysningsloven, inkludert personvernforordningen, forskrift til opplæringsloven, *Instruks for virksomhetsstyring i Oslo kommu*ne, *Instruks for informasjonssikkerhet i Oslo kommune* og *Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet i Oslo kommune.*

Forvaltningsrevisjonen har vært innrettet for å revidere praksis for behandling av elevenes personopplysninger ved to utvalgte skoler: Hauketo skole og Nordseter skole. Undersøkelsen omfatter i tillegg en del om Utdanningsetaten sentralt sitt arbeid på flere områder, da det er en viktig del av rammene for skolenes arbeid, og oppgaver som ellers hadde ligget til den enkelte skole. Undersøkelsen er gjennomført med intervjuer og gjennomgang av dokumentasjon. I tillegg har Kommunerevisjonen blitt vist hvordan ulike prosesser ved de to skolene ble gjennomført.

Data har i hovedsak blitt samlet inn mellom mai og september 2022. Undersøkelsesperioden har i utgangspunktet vært skoleåret 2020/2021 og skoleåret 2021/2022, men på en rekke punkter har det vært naturlig å beskrive praksis på observasjonstidspunktet.

I det følgende presenteres Kommunerevisjonens sentrale vurderinger.

Sentrale vurderinger

Kartlegging av informasjonsverdier og risikovurdering og -håndtering

Hauketo skole og Nordseter skole hadde i noen grad oversikt over sin behandling av elevenes personopplysninger i systemer, apper og nettjenester gjennom dokumentasjon som Utdanningsetaten sentralt hadde utarbeidet. Etaten hadde også gjennomført enkelte personvernkonsekvensvurderinger og flere risikoanalyser. Etaten hadde ikke ferdigstilt personvernkonsekvensvurderinger for læringsteknologien som var i bruk i Osloskolen, men arbeidet med dette. Det var en mangel at IST Everyday ble tatt i bruk før personvernkonsekvensvurderingen var gjennomført.

De undersøkte skolene hadde ikke gjort vurderinger av om oversiktene Utdanningsetaten hadde utarbeidet, var dekkende for skolens bruk. Skolene hadde heller ikke dokumentert vurderinger av om det var risikoer forbundet med måten skolene benyttet systemene. Skolene hadde ikke gjennomført personvernkonsekvensvurderinger blant annet knyttet til utarbeiding av individuelle opplæringsplaner som omfattet særlige kategorier personopplysninger. Disse dokumentene ble behandlet i systemer som ikke var godkjent for slike personopplysninger. Det var også risiko for at skolene behandlet sensitive elevopplysninger i e-post, noe som forekom ved begge skolene. Kommunerevisjonen merker seg at Utdanningsetaten var kjent med at skolene manglet et verktøy for samhandling mellom ledelse og lærere for behandling av særlige kategorier personopplysninger. Etaten oppga at den hadde igangsatt et langsiktig arbeid med anskaffelse av et slikt verktøy.

Nordseter skole og andre skoler som brukte iPad, benyttet Showbie, et system hvor elevers personopplysninger ble behandlet. Kommunerevisjonen stiller spørsmål ved at Utdanningsetaten ikke hadde gjennomført en fullstendig personvernkonsekvensvurdering av systemet Showbie, ettersom systemet inneholder læreres vurdering av elevarbeider.

Tilgangsstyring

Både Hauketo skole og Nordseter skole hadde rutiner som var egnet til å sikre at skolen hadde oversikt over de ansattes tilganger til informasjon i sentrale digitale systemer. Dette ga også mulighet til å sikre at tilgangene var i samsvar med tjenstlig behov. Ved begge skolene var det likevel svakheter i rutinene for å sikre at tilganger ble avsluttet i løpet av et skoleår, når det tjenstlige behovet falt bort. Undersøkelsen tyder på at begge skolene hadde oversikt over hvem som hadde adgang til fysiske arkiv, der eldre elevmapper ble oppbevart.

Lærerne ved skolene hadde imidlertid ikke tilgang til skolens saks- og arkivsystem Websak, der elevmappene lå. Dette ga skolene utfordringer med å sikre lærerne tilstrekkelig tilgang til personopplysninger om elevene og tilgang til et sikkert sted å behandle slike opplysninger digitalt. Dette kan ha bidratt til en praksis ved begge de undersøkte skolene der lærere som ikke hadde tjenstlig behov, hadde tilgang til elevers

individuelle opplæringsplaner o.a. i et system som ikke var godkjent for behandling av særlige kategorier personopplysninger.

Forsøk på anonymisering av elever ved bruk av initialer, forekom ved begge skolene, blant annet i individuelle opplæringsplaner og årsrapporter. Kommunerevisjonen mener det er høy risiko for at ansatte uten tjenstlig behov kunne identifisere elevene også når navnet ikke framgikk, og vil peke på at det er risiko for at disse dokumentene kunne inneholde særlige kategorier personopplysninger og andre sensitive opplysninger. Undersøkelsen tyder på at det kunne variere om utskrifter av dokumentasjon ble oppbevart på en slik måte at det kun var lærere med tjenstlig behov som hadde adgang.

Opplæring og kompetanse

Hauketo skole hadde ikke sikret tilfredsstillende opplæring i personvern for de ansatte ved skolen. Kommunerevisjonen stiller også spørsmål ved om opplæringen ved Nordseter skole var tilstrekkelig til å sikre alle ansatte tilfredsstillende kompetanse.

Avvikshåndtering

Verken Hauketo skole eller Nordseter skole hadde etablert tilfredsstillende rutiner og praksis for avvikshåndtering. Kommunerevisjonen merker seg at Hauketo skole hadde fanget opp svært få personvernavvik, og stiller spørsmål ved om dette reflekterer det reelle antallet avvik. Kommunerevisjonen ser alvorlig på at det gikk nesten tre uker fra Nordseter skole fikk opplysninger om systematisk svake Feide-passord for en del elever, før skolen iverksatte tiltak.

Mangelfulle rutiner og praksis ga risiko for at personvernavvik på de to skolene ikke ble fanget opp, forsvarlig lukket og fulgt opp.

Anbefalinger

Kommunerevisjonen anbefaler at begge skolene iverksetter tiltak for å

- sikre at den har oversikt over sin behandling av personopplysninger, og at den gjennomfører nødvendige risikovurderinger og personvernkonsekvensvurderinger, når dette ikke er gjort av Utdanningsetaten sentralt
- sikre at tilgang til elevers personopplysninger er i tråd med tjenstlig behov
- sikre at ansatte har tilfredsstillende kompetanse når det gjelder ivaretakelse av elevers personvern
- sikre at personvernavvik blir tilfredsstillende håndtert, herunder fanget opp, lukket og fulgt opp

Utdanningsetaten sentralt utfører oppgaver knyttet til personvern og informasjons-sikkerhet som ellers ville ha ligget til den enkelte skole. Etatens arbeid er en viktig del av rammene for skolenes arbeid på området. Kommunerevisjonen anbefaler at Utdanningsetaten

- legger til rette for at skolene kan behandle særlige kategorier personopplysninger og andre sensitive personopplysninger på en tilfredsstillende måte, herunder i samhandlingen mellom lærere og ledelse
- viderefører arbeidet med å sikre at elevers personopplysninger ivaretas i Osloskolen
- følger opp de undersøkte skolenes forbedringsarbeid knyttet til deres behandling av elevers personopplysninger

Kommunerevisjonen anbefaler at byråden for oppvekst og kunnskap følger opp Utdanningsetatens forbedringsarbeid knyttet til etatens behandling av elevers personopplysninger.

Uttalelser til rapporten

Kommunerevisjonen har mottatt uttalelser til rapporten fra byråden for oppvekst og kunnskap, Utdanningsetaten, Hauketo skole og Nordseter skole. Etaten og de to skolene avga en felles uttalelse. Kommunerevisjonen har sammenfattet og vurdert uttalelsene i kapittel 8, og gjengitt disse i sin helhet i vedleggene 3 og 4. Utdanningsetaten, skolene og Byrådsavdeling for oppvekst og kunnskap har varslet eller iverksatt tiltak. Deriblant vil etaten gå grundig gjennom anbefalingene i rapporten og lage en prioritert oppfølgingsplan.

1. Innledning

1.1 Bakgrunn

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger (Datatilsynet, 2019). Personvernlovgivningen stiller blant annet krav til hvordan personopplysninger skal behandles og sikres. I 2018 ble nye personvernregler innført i hele EU/EØS, noe som innebar at disse rettighetene ble ytterligere styrket. Personvernforordningen ble gjennomført i Norge i en ny personopplysningslov, som trådte i kraft i juli 2018.

Personopplysninger er i personvernforordningen definert som enhver opplysning om en identifisert eller identifiserbar person. Dette kan for eksempel være navn, adresse, fødselsnummer, bilder der personer kan gjenkjennes mv. Etter personopplysningsloven stilles det særlige krav til behandling av såkalte særlige kategorier av personopplysninger (sensitive personopplysninger), slik som helseopplysninger, opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, seksuell legning og seksuelle forhold.

Alle skoler behandler en mengde personopplysninger om elevene. Dette omfatter for eksempel opplysninger om fravær, anmerkninger, familieforhold, helse, eventuelle lærevansker mv. Utdanningsetaten har også ansvar for mange systemer med et stort antall brukere, både læringsteknologiske systemer og administrative systemer. Dersom Utdanningsetaten og skolene ikke har tilfredsstillende rutiner og praksis for håndtering av personopplysninger, kan det blant annet medføre at informasjon kommer på avveie eller går tapt.

Det er ifølge Datatilsynet særlig to hovedutfordringer i skolesektoren som gjelder for nær sagt alle kommuner. For det første har skolenes digitale kompetanse ikke holdt tritt med tempoet i digitaliseringen. Videre er kommunene ofte ikke i stand til å beskytte sine mest sårbare innbyggeres personvern godt nok. Det har også framkommet flere eksempler på svakheter og mangler ved kommuners og skolers ivaretakelse av personvernet til elevene og familiene deres. I september 2018 førte et avvik knyttet til mobilapplikasjonen Skolemelding, som gjorde det mulig å få tilgang til personopplysninger om elever, til at Datatilsynet i april 2019 ila Oslo kommune et overtredelsesgebyr på 1,2 millioner kroner. Utdanningsetaten lukket sikkerhetshullet da det ble avdekket, og har senere gjennomført en rekke tester av sikkerheten i Skolemeldingsappen. Koronapandemien og hjemmeundervisning medførte nye problemstillinger for skolesektoren knyttet til personvern.

Kommunerevisjonen har i flere undersøkelser berørt tematikken informasjonssikkerhet i skole. Rapport 2/2021 *Forebygging og oppfølging av mobbing og vold*, avdekket blant annet svakheter knyttet til tilgangsstyring, skriftlig risikovurdering, samt at Utdanningsetaten hadde lagt opp til en praksis som innebar at skoler ved varsling om alvorlige saker i enkelte tilfeller hadde oversendt personopplysninger som kan være sensitive,[1] per e-post. I rapport 7/2020 *Forebygging av frafall fra videregående*

[1] Med begrepet «sensitive», menes i denne sammenheng særlige kategorier personopplysninger, slik som helseopplysninger, og andre personopplysninger som har

opplæring fant Kommunerevisjonen at det var elementer av god praksis for tilgangsstyring som de to undersøkte skolene ikke fulgte. Videre var Utdanningsetaten case i rapport 1/2019 *Sikkerhetskrav i anskaffelser*, som blant annet viste at etaten ikke hadde utarbeidet risikoanalyser forut for kravspesifikasjon for de undersøkte anskaffelsene, samt svakheter knyttet til kontroll og testing av sikkerhetskrav.

1.2 Formål og problemstillinger

Formålet med forvaltningsrevisjonen har vært å bidra til å sikre at skolenes behandling av personopplysninger om elevene er i samsvar med personvernlovgivningen.

Problemstillingen har vært følgende:

- Er personopplysninger om elever tilstrekkelig sikret i skolene?

For å undersøke problemstillingen, har vi undersøkt følgende undertemaer:

- kartlegging av informasjonsverdier og risikovurdering og -håndtering
- tilgangsstyring
- opplæring og kompetanse
- avvikshåndtering

1.3 Avgrensninger

Forvaltningsrevisjonen har vært innrettet for å se på praksis ved de utvalgte enkeltskolene, som er Hauketo skole og Nordseter skole. Undersøkelsen omfatter likevel en del om arbeidet til Utdanningsetaten sentralt på flere områder, da dette arbeidet er en viktig del av rammene for skolenes arbeid og omfatter oppgaver som ellers hadde ligget til den enkelte skole.

Vi har ikke spesifikt undersøkt hvordan elevenes personvern ble ivaretatt i løsningene for hjemmeundervisning under koronapandemien. Vi har videre ikke undersøkt ivaretakelsen av personvern ved skolenes samhandling med andre aktører, for eksempel skolehelsetjenesten, PPT (Pedagogisk-psykologisk tjeneste) eller barnevernet, særskilt.

1.4 Revisjonskriterier

Revisjonskriteriene er målestokken som ligger til grunn for Kommunerevisjonens vurderinger. I denne forvaltningsrevisjonen er kriteriene i hovedsak utledet fra

- personopplysningsloven, inkludert personvernforordningen
- forskrift til opplæringsloven
- byrådssak 1070/15 *Instruks for virksomhetsstyring i Oslo kommu*ne
- byrådssak 1105/13 *Instruks for informasjonssikkerhet i Oslo kommune*
- byrådssak 1099/10 *Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet i Oslo kommune*
- veiledning fra Datatilsynet

Vi presenterer revisjonskriteriene løpende i kapittel 3–6 og gir en samlet framstilling, inkludert utledning, i vedlegg 1.

behov for særskilt konfidensialitetsbeskyttelse, herunder opplysninger om elevens personlige forhold.

1.5 Metodisk tilnærming og gjennomføring

Forvaltningsrevisjonen bygger på gjennomgang av dokumentasjon fra Utdanningsetaten og fra de to undersøkte skolene. Videre har vi gjennomført intervjuer med sentrale ansatte ved de to skolene, herunder representanter for ledelsen, IKT-ansvarlig, kontorpersonell, rådgivere og lærere. Vi har også blitt vist hvordan ulike prosesser som omfatter elevers personopplysninger, gjennomføres i de to skolenes IKT-systemer.

Undersøkelsesperioden har i utgangspunktet vært skoleåret 2020/2021 og skoleåret 2021/2022, men på en rekke punkter har det vært naturlig å beskrive praksis på observasjonstidspunktet.

En mer utfyllende beskrivelse av metodisk tilnærming og gjennomføring gis i vedlegg 2.

1.6 Rapportens oppbygging

I kapittel 2, som er et beskrivende kapittel, presenterer vi kortfattet sentrale forhold ved Utdanningsetatens styringssystem for informasjonssikkerhet og personvern samt de to skolene som omfattes av undersøkelsen. Kapittel 3 handler om skolenes kartlegging av informasjonsverdier, risikovurdering og risikohåndtering. Kapittel 4 omhandler skolenes styring av tilgang til personopplysninger. I kapittel 5 vurderer vi arbeidet for å sikre tilstrekkelig opplæring og kompetanse knyttet til ivaretakelse av personvern. Kapittel 6 handler om håndtering av avvik knyttet til elevers personopplysninger. I kapittel 7 er våre konklusjoner og anbefalinger. I kapittel 8 har vi oppsummert og vurdert vesentlige momenter i uttalelsene fra byrådsavdelingen, Utdanningsetaten og de to skolene. Undersøkelsens revisjonskriterier og grunnlaget for dem er lagt i vedlegg 1, mens det er redegjort nærmere for undersøkelsens metode og framgangsmåte i vedlegg 2. De mottatte uttalelsene følger i sin helhet som vedlegg 3 og 4.

2. Sentrale forhold ved Utdanningsetatens styringssystem og de undersøkte skolene

2.1 Styringssystem for informasjonssikkerhet og personvern

Utdanningsetaten hadde utarbeidet et styringssystem for informasjonssikkerhet og personvern. Styringssystemet var tilgjengelig på Utdanningsetatens intranett, Tavla, og inneholdt en rekke styrende dokumenter. Det framkom at styringssystemet var midlertidig godkjent i perioden 15. januar–31. mars 2021. Denne versjonen av styringssystemet lå tilgjengelig på Tavla per ultimo oktober 2022, og Kommunerevisjonen fikk opplyst fra etaten at dokumentene i systemet var gjeldende.

Styringssystemet inneholdt blant annet policy for informasjonssikkerhet og personvern, instrukser for ansatte i skolen, instruks for avvikshåndtering innen informasjonssikkerhet og personvern, instruks for personvern, instruks for roller og ansvar, instruks for tilgangsstyring m.m. Enkelte av disse dokumentene vil bli nærmere redegjort for senere i rapporten.

2.2 Roller og ansvarsfordeling

I Utdanningsetatens instruks for rolle og ansvar innen informasjonssikkerhet og personvern ble ansvaret til ulike roller i etaten beskrevet. Direktøren i Utdanningsetaten hadde det helhetlige ansvaret for informasjonssikkerhet og personvern i etaten, inkludert i administrasjonen og på skoler. I tillegg framkom informasjon om andre roller i arbeidet, blant annet informasjonssikkerhetskoordinator og personvernkoordinator.

Det framkom at rektor hadde operativt ansvar for å ivareta informasjonssikkerhet og personvern på sin skole. Dette innebar at rektor skulle

- sikre at prosesser og systemer (tjenester) levert ut på skoler er i samsvar med lov, regelverk og kravene til informasjonssikkerhet og personvern iht. Utdanningsetatens policy og instrukser
- sikre at det gjennomføres årlig overordnet risikovurdering for skoler
- sikre at alle ansatte på skolen har gjennomført opplæring for informasjonssikkerhet og personvern
- sikre at alle avvik innen informasjonssikkerhet og personvern rapporteres til Utdanningsadministrasjon
- måle etterlevelse av krav til informasjonssikkerhet og personvern

For å øke fokus på informasjonssikkerhet og personvern på skolene skulle hver skole også ha en informasjonssikkerhetskontakt. Informasjonssikkerhetskontaktens oppgaver omfattet ifølge instruksen blant annet å bistå rektor med å gjennomføre oppgavene innenfor informasjonssikkerhet og personvern.

Skoleplattform Oslo

Det framgikk av Utdanningsetatens nettsider at etatens digitale løsninger for elever, ansatte og foresatte var samlet i en felles plattform som het Skoleplattform Oslo. Med Skoleplattform Oslo mentes IKT-systemer og aktiviteter for administrering, planlegging, gjennomføring og oppfølging av undervisningen i Osloskolen. Løsningene skulle legge til rette for kommunikasjon og samarbeid i Osloskolen. Skoleplattform Oslo ga tilgang til informasjon og relevante arbeidsverktøy for lærere, elever og foresatte.

2.3 Om skolene i undersøkelsen

2.3.1 Hauketo skole

Hauketo skole er en ungdomsskole i Bydel Søndre Nordstrand, med om lag 330 elever. Skolen hadde også en byomfattende avdeling for inntil 12 elever med autismespekterdiagnose. Alle elevene på skolen hadde PC-er. I tillegg hadde skolen et klassesett med iPader, som ifølge skoleledelsen i liten grad ble brukt.

2.3.2 Nordseter skole

Nordseter skole er en 1–10-skole i Bydel Nordstrand. Skolen hadde om lag 1100 elever og over 120 ansatte. Skolen hadde høsten 2016 gått fra å være en ungdomsskole til å bli kombinert barne- og ungdomsskole. Alle elevene på skolen hadde tidligere hatt en egen iPad. Fra skoleåret 2022–2023 skulle elevene på 8.–10. trinn over på PC og skulle i tillegg ha delte iPader. Våren 2022 var det full PC-dekning på 10. trinn.

3. Kartlegging av informasjonsverdier og risikovurdering og -håndtering

3.1 Revisjonskriterier

Kommunerevisjonen har lagt følgende revisjonskriterier til grunn:

- Skolen skal ha oversikt over sin behandling av elevenes personopplysninger. Oversikten skal være dokumentert.
- Sannsynlige personvernkonsekvenser skal vurderes før behandling starter. Vurderingen skal være dokumentert. Dersom det er sannsynlig at behandlingen kan medføre høy risiko, skal dette gjøres i form av en personvernkonsekvensvurdering (DPIA – Data Protection Impact Assessment).
- Risikoen for informasjonssikkerhetshendelser knyttet til behandling av personopplysninger om elever skal vurderes. Risikovurderingen skal være dokumentert.

Vi har lagt til grunn at de ovennevnte prosessene kan ivaretas av enten Utdanningsetaten sentralt eller av de enkelte skolene.

3.2 Faktabeskrivelse

Kommunerevisjonen reviderer de to utvalgte skolenes behandling av personopplysninger. Vurderinger og oversikter utarbeidet av Utdanningsetaten er en del av rammebetingelsene for skolens behandling og er derfor relevant for å vurdere om den enkelte skole har kontroll på personvernrisikoen. Dette kapittelet inneholder derfor først en beskrivelse av Utdanningsetatens behandlingsoversikter, risikovurderinger mv. Deretter følger faktabeskrivelser for skolene.

3.2.1 Utdanningsetaten

Behandlingsoversikter

Utdanningsetaten hadde utarbeidet ulike dokumenter med oversikt over behandling av personopplysninger i etaten. Dette omfattet en overordnet behandlingsoversikt med informasjon om blant annet hvilken type personopplysninger som ble behandlet i ulike virksomhetsprosesser. Virksomhetsprosesser som omfattet elevopplysninger var:

- saksbehandling og arkiv
- kontorstøtte for administrasjonsansatte
- kontorstøtte for elever og lærer (skoleplattform)
- undervisning/pedagogisk (skoleplattform)
    - lagring i Norge
- undervisning/pedagogisk (skoleplattform)
    - lagring utenfor Norge
- kommunikasjon og samhandling (skoleplattform)
- fagopplæring
- elevforvaltning grunnskole / videregående opplæring
- skoleskyss

I tillegg var IKT-Drift omtalt, men her framgikk det ingen andre opplysninger enn hvilke IT-systemer som ble benyttet.

Oversikten ga blant annet informasjon om hvilken kategori personopplysninger som ble behandlet (alminnelige eller særlige kategorier jf. omtale i kapittel 1), og om det gjaldt ansatte, elever og/eller foresatte, hva som var det rettslige behandlingsgrunnlaget for behandlingen, og hvilke IKT-systemer som ble benyttet. Oversikten var godkjent av Utdanningsdirektøren 15. mars 2022.

For to prosesser, *Saksbehandling og arkiv* og *Skoleskyss*, framgikk det at behandlingen av særskilte kategorier personopplysninger foregikk i saks- og arkivsystemet Websak. For de øvrige prosessene (unntatt IKT-drift) ble det ifølge oversikten behandlet alminnelige personopplysninger.

Etaten hadde også en behandlingsoversikt per IKT-system, som gjaldt fram til mars 2022, som omfattet følgende systemer som behandlet elevopplysninger:

- Websak
- Adminplattform (Active Directory, Microsoft Exchange, SMS Passcode), Personal- og ressurskatalogen (PRK)
- Office 365, Sikt basistjenester (inkl. driftsportalen), Skoleplattform Oslo, Feide[2], LSI
- SATS, IST Everyday, SITS, Vigo-OT
- Visma Flyt PPT
- Itslearning, Conexus Engage, Prøveplattform Oslo
- Elevskyss
- Vigo Fag
- Skolemeldingsapp, CorePublish, Portalen.

Det framkom i oversikten at det ble behandlet særlige kategorier personopplysninger om elever i ett av systemene. Dette var Visma Flyt PPT. For *Skolemeldingsapp, CorePublish* og *Portalen* var det opplyst om at slike opplysninger ikke ble behandlet, men at det var mulig for brukerne å legge inn for eksempel helseopplysninger i fritekstfelt. Oversikten var godkjent av sikkerhetsleder og var ifølge endringsloggen sist oppdatert i desember 2018.

Disse behandlingsoversiktene var ikke tilgjengelig for skolene på Utdanningsetatens intranett.

Også i Utdanningsetatens personvernerklæringer framkom det informasjon om hvilke personopplysninger som ble behandlet i etatens IT-systemer.

Informasjon om behandling av personopplysninger i personvernerklæringer

I sin generelle personvernerklæring[3] ga Utdanningsetaten overordnet informasjon om sin behandling av elevers, foresattes og ansattes personopplysninger. Det framgikk at etaten brukte ulike digitale læremidler for å gi elevene opplæring, vurdering og bedre tilpasset opplæring, og at læremidlene skulle være vurdert og godkjent for bruk, for å sikre at Osloskolen ivaretok personvernet. Erklæringen ga også en beskrivelse av, og eksempler på, personopplysningene som ble behandlet, og lenket til underliggende

[2] Feide står for Felles Elektronisk IDEntitet og er den nasjonale løsningen for sikker innlogging og datadeling i utdanning og forskning (kilde: https://aktuelt.osloskolen.no/larerik-bruk-av-laringsteknologi/informasjonssikkerhet-og-personvern/feide-tjenester/)

[3] https://aktuelt.osloskolen.no/personvernerklaring-for-osloskolen/personvernerklaring/personvernerklaring1/

personvernerklæringer knyttet til de enkelte IT-systemene. Disse var organisert under temaene *Behandling av elevopplysninger*, *Behandling av foresatteopplysninger* og *Behandling av ansatteopplysninger* og hadde versjonsdatoer i mars eller juni 2022. Oversikten over systemer der elevers personopplysninger ble behandlet, omfattet følgende systemer:

- Portalen og Skolemelding
- Office 365
- Itslearning (læringsplattform)
- IST Everyday (skoleadministrativt system)
- Visma InSchool (skoleadministrativt system)
- SITS (fagsystem for Oslo Voksenopplæring)
- Vigo Opplæring (Inntak og fagopplæring) og Vigos webmoduler
- Conexus Engage (samler prøver og kartlegginger for elever i grunnskolen)
- Inspera Assessment (Prøveplattform Oslo)
- Driftsportalen
- Lærerstyrt internett

I de systemspesifikke personvernerklæringene ble det gjort rede for ulike sider ved behandlingen av personopplysninger, som hva slags opplysninger som ble behandlet, hva som var formålet med behandlingen, og det rettslige behandlingsgrunnlaget.

IST Everyday er det skoleadministrative systemet for grunnskolen i Oslo. For dette systemet framgikk det i personvernerklæringen blant annet at systemet ga prosesstøtte for både sentrale og lokale arbeidsoppgaver i skolehverdagen og skoleledelse samt for administrasjon av lærere, elever og foresatte, og at grunnlaget for behandling av personopplysninger i det skoleadministrative systemet var opplæringsloven med forskrift og forvaltningsloven. Det ble opplyst om at ingen sensitive personopplysninger skulle registreres i systemet. Videre ble det listet opp en rekke typer personopplysninger om eleven som ble behandlet, herunder om fravær, faglig progresjon, orden og atferd og skolerelaterte behov og ferdigheter. Det framgikk også at informasjon om særskilt norskopplæring og individuell opplæringsplan ble behandlet i systemet.

Office 365 er det daglige arbeidsverktøyet for elever og ansatte i Osloskolen til produksjon, lagring og deling av data. I personvernerklæringen ble det gjort rede for personopplysninger som knyttes til den enkelte bruker av systemet, i tillegg til at det framgikk at systemet også ville inneholde brukernes egenproduserte materiale, som kunne inneholde personopplysninger, og at disse potensielt kunne lagres på fellesområder. Det framgikk videre at det var IKT-ansvarlig ved skolene som organiserte fellesområder og bidro til oppsett av kontorstøtte- og samhandlingsverktøy som Microsoft SharePoint, OneNote og Teams. Utdanningsetaten hadde ikke ferdigstilt personvernvurdering for Microsoft-universet, men i etatens utkast (versjon 0.91) sto følgende:

> Aktivitetsdata skal i skolesammenheng ikke omfatte private opplysninger av typen adresse, opplysninger om økonomi, bekjentskapskrets, eller liknende. Denne informasjonen samles kun inn dersom brukeren selv har lagt inn denne informasjonen, og det skal unngås. Det er også tilfeller hvor leverandøren logger lokasjonsdata fra brukeren (basert på hvor enheten er), men dette kan man som oftest skru av funksjonalitet for.

> Aktivitetsdata av særskilte kategorier av personopplysninger, som for eksempel opplysninger om helse, rase og religion (forordningens artikkel 9) skal begrenses. Tilfeller hvor dette gjøres, er det retningslinjer for hvordan og dette inkluderer anonymisering, tilgangsstyring og sletting.

Utdanningsetaten opplyste om at den manglet et samhandlingsverktøy, for eksempel mellom ledelsen på en skole og lærerne, for å behandle særlige kategorier av personopplysninger. Etaten hadde igangsatt et langsiktig arbeid med å anskaffe et slikt verktøy, men mangelen var et problem på kort sikt. Etaten pekte på at noen skoler hadde benyttet Teams eller OneNote til dette, men at dette ikke var egnet på grunn av sannsynligheten for brukerfeil, og videre at etaten ikke hadde godkjent Teams eller OneNote for behandling av særlige kategorier personopplysninger. Etaten opplyste om at den hadde startet risikovurdering av Teams og OneNote for å redusere risikoen for at skolene, i mangel av funksjonelle og sikre samhandlingsløsninger, tok i bruk ikke-godkjente løsninger.

I Utdanningsetatens sikkerhetsinstruks for ansatte i skolene, sto det at dersom e-post måtte benyttes for overføring av beskyttelsesverdig informasjon, skulle informasjonen sendes som kryptert vedlegg til e-post med godkjent krypteringsprogram. Videre, ved mottak av beskyttelsesverdig informasjon via e-post, skulle anonymisering vurderes ved eventuell videresendelse av e-post. Innholdet i en slik e-post skulle overføres til et sikkert lagringssted, for eksempel elevmappen eller sikker sone, før den mottatte e-posten skulle slettes.

Informasjon om behandling av personopplysninger i digitale læremidler

Utdanningsetatens generelle personvernerklæring ga, som nevnt ovenfor, noe overordnet informasjon om etatens bruk av digitale læremidler. I tillegg var det lenket til et eget dokument om personvern i digitale læremidler, delt inn i Feide-tjenester, iPad-apper, Microsoft-tjenester og Andre webtjenester. Innenfor hvert av disse «universene» var det listet opp tjenester Utdanningsetaten hadde godkjent for bruk, og tjenester som var vurdert, men ikke godkjent.

I listene over godkjente tjenester var det for de aller fleste tjenestene lenket til en side med informasjon om tjenesten, herunder om den behandler personopplysninger, og i så fall hvilke, samt informasjon om eventuelle forutsetninger for bruk av tjenesten. For digitale læremidler med Feide-innlogging var det (per 30.09.2022) lenke til informasjon om 35 av 75 tjenester, for iPad-tjenester (per 22.09.2022) om 58 av 59 tjenester og for andre webtjenester (per 19.09.2022) om 14 av 14. For Microsoft-tjenester (per 23.09.2022) var det lenket til etatens personvernerklæring for Office 365 der det, som nevnt over, ble gjort rede for hvilke personopplysninger som behandles. I tillegg ble det informert om at:

> Microsoft sine tjenester skal ikke benyttes til personopplysninger av sensitiv art som kan knyttes direkte til enkeltperson. I noen tilfeller vil det være nødvendig for lærerne å notere ned informasjon om elever, da skal skolen ha retningslinjer for hvordan dette skal gjøres uten å avsløre elev.
>
> Microsoft sine tjenester er ikke et samhandlingsverktøy mellom skole og hjem. Dette er det egne rutiner og tjenester for.

Videre var Minecraft (onlinespill) med som godkjent tjeneste via Microsoft fordi elevenes Microsoft-konto brukes for pålogging. Det var ikke lenket til side med ytterligere informasjon om Minecraft.

Personvernvurderinger og risikovurderinger

Utdanningsetaten utarbeidet i 2020 en personvernkonsekvensvurdering for behandlingen av elevopplysninger i det skoleadministrative systemet IST Everyday. Det framgår av dokumentet at Oslo kommunes personvernombud hadde lest og kommentert rapporten. Personvernkonsekvensvurderingen ble godkjent i november 2020. IST Everyday ble ifølge Utdanningsetatens årsberetning for 2020 tatt i bruk i grunnskolen i august 2020.

Etaten begrunner vurderingen av at det var høy risiko med at bruken av systemet innebar behandling av barns personopplysninger i stor skala, og at elevopplysninger var av en art som var inkludert i Datatilsynet liste[4] over behandlingsaktiviteter som alltid krever at det gjennomføres en personvernkonsekvensvurdering. Datatilsynets liste omfatter blant annet «Behandling av personopplysninger for å evaluere læring, mestring og trivsel i skoler eller barnehager».

En rekke apper og nettjenester er i bruk som digitale læremidler i Osloskolen. Utdanningsetaten startet i november 2020 et arbeid med å lage vurderinger av personvernkonsekvenser for bruken av disse, som i løpet av flere år hadde blitt tatt i bruk av osloskoler. Det var nedsatt en egen personverngruppe som sto for dette arbeidet. Arbeidet var organisert på tre nivåer, gjennom en overordnet personvernkonsekvensvurdering av personvern i digitale læremidler og supplerende overordnede personvernkonsekvensvurderinger for de tre «universene» iPad, Feide og Microsoft. Det framgikk av disse at vurderingene kunne brukes som grunnlag for risikovurderinger og personvernkonsekvensvurderinger av tjenester og apper. De fire overordnede personvernkonsekvensvurderingene var per september 2022 ikke ferdigstilt og lå ifølge etaten til språkvask i kommunikasjonsavdelingen.

I tillegg til å utarbeide de overordnede personvernkonsekvensvurderingene, skulle personverngruppa, ifølge etaten, lage risiko- og sårbarhetsanalyser (ROS) for de enkelte appene/verktøyene som er felles for Osloskolen. Det framgår også av etatens utkast til *Overordnet vurdering av personvern i digitale læremidler* at etaten skal gjennomføre risiko- og sårbarhetsanalyser som ledd i prosessen med å godkjenne en tjeneste eller app. Dette var for at den enkelte skole ikke selv skulle trenge å vurdere om disse kunne benyttes. Som del av ROS-analysene skulle det vurderes om det var høy risiko for de registrertes personvernrettigheter og -friheter, slik at det var behov for en full personvernkonsekvensvurdering.

Som nevnt ovenfor var personverngruppas oppgaver i hovedsak knyttet til vurderinger av læringsteknologi i form av apper og nettjenester som var i bruk, eller som skoler ønsket å ta i bruk. Ifølge Utdanningsetaten skulle alle risikovurderinger av informasjonssikkerheten i de ulike systemene ajourholdes minst årlig.

Kommunerevisjonen har innhentet eksempler på dokumentasjon fra gjennomførte risikovurderinger, blant annet av ulike prosesser i Office 365-verktøyene Teams, SharePoint og OneNote og av appen og portalen for Skolemelding. I tillegg framgikk

[4] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/

resultater fra risikoanalyser av det skoleadministrative systemet IST Everyday i personvernkonsekvensvurderingen for dette systemet omtalt ovenfor.

Utdanningsetaten rapporterer årlig status på informasjonssikkerhets- og personvernområdet – herunder for gjennomføring av risikovurderinger og personvernkonsekvensvurderinger – til Byrådsavdeling for oppvekst og kunnskap. I rapporten for perioden september 2021 til og med august 2022 rapporterte etaten blant annet om gjennomført risikovurdering av Skoleplattformen. Etaten pekte videre på at brukere etterspurte verktøy som kunne benyttes til å kommunisere sensitive personopplysninger. Anskaffelse av verktøy for sikker deling av elevopplysninger var blant aktivitetene etaten rapporterte at den ønsket å prioritere i neste rapporteringsperiode.

Kommunerevisjonen har mottatt en risiko- og sårbarhetsanalyse av en app i iPad-universet. Dette gjaldt læringsplattformen Showbie, som – ifølge ROS-analysen og etatens informasjonsside[5] om Showbie – var en læringsplattform for undervisningsaktiviteter og inneholdt verktøy for planlegging, elevaktivitet, vurdering og oppfølging. Appen ga også foresatte mulighet til å følge opp barnets arbeid og lærernes vurdering av dette. Analysen omfattet en «mini-personvernkonsekvensvurdering», det vil si en vurdering av om det var behov for en full personvernkonsekvensvurdering. Etaten vurderte at det ikke var behov for det, men at den overordnede personvernkonsekvensvurderingen var dekkende, det vil si utkastet til overordnet personvernkonsekvensvurdering for iPad-universet, nevnt ovenfor. Utdanningsetaten opplyste at Showbie fram til sommeren 2022 hadde serverne sine, og dermed behandlet personopplysninger, i USA. Serverne ble da flyttet til Stockholm. Flyttingen av datasenteret fra USA til Stockholm var også omtalt i ROS-analysen nevnt over. Utdanningsetaten oppga at den hadde kontraktsfestet avtale om Showbies behandling av personopplysninger i USA med gyldig overføringsgrunnlag gjennom EU-kommisjonens standard personvernbestemmelser (Standard Contractual Clauses), som ble vedtatt 4. juni 2021.[6]

ROS-analysene for de enkelte appene/verktøyene var ifølge lederen for personverngruppa arkivert i Websak. I tillegg lå det informasjon på etatens internettsider (aktuelt.osloskolen.no) om verktøyene/appene som var vurdert, blant annet om retningslinjer/forutsetninger for bruk. Det var ifølge lederen for gruppa et poeng at informasjonen ikke bare skulle være tilgjengelig for lærere, men også for elever, foreldre, leverandører mfl., og at informasjonen skulle være oppdatert når det gjelder status.

Det var utarbeidet oversikter over verktøy som var vurdert og godkjent i fire «univers»: Feide, Microsoft, iPad og Andre webtjenester. I tillegg fantes det en oversikt over ikke-godkjente verktøy. Det lå informasjon om mange av de ulike verktøyene som var omfattet av oversiktene, på Utdanningsetatens nettsider (aktuelt.osloskolen.no), slik at informasjonen var tilgjengelig for skolene, men også for elever, foresatte og

[5] https://aktuelt.osloskolen.no/larerik-bruk-av-laringsteknologi/informasjonssikkerhet-og-personvern/ipad-apper/ og https://aktuelt.osloskolen.no/larerik-bruk-av-laringsteknologi/informasjonssikkerhet-og-personvern/ipad-apper/showbie/

[6] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
Kommunerevisjonen har ikke undersøkt hva som var overføringsgrunnlaget før denne avtalen ble inngått.

leverandører. På observasjonstidspunktet gjaldt det alle godkjente iPad-apper og «Andre webtjenester». For Feide-universet var det lenket til informasjon om 35 av 80 digitale læremidler og 11 av 38 administrative verktøy. Etaten opplyste at den prioriterte de mest brukte og/eller kritiske appene. Per mai 2022 var etaten om lag halvveis i arbeidet med å vurdere enkeltapper og planla å være ferdig med størstedelen av etterslepet i løpet av 2022.

Det var delegert til skolene å avgjøre hvilke læremidler de skulle bruke. Utdanningsetaten opplyste at etaten gjennom blant annet arbeidet omtalt over laget rammer som la til rette for lovetterlevelse i skolene. Videre opplyste etaten om at rektor var ansvarlig for å vurdere om bruken var i tråd med regelverket, hvis skolene tok i bruk apper eller nettjenester som ikke var vurdert av Utdanningsetaten ved personverngruppa. På Utdanningsetatens internettsider sto det imidlertid at det var skoleeier som godkjente tjenestene for bruk, og at det også var skoleeier som inngikk databehandleravtale med leverandører. Det framgikk videre at skoler som ønsket å ta i bruk nye tjenester og apper, kunne bestille personverngodkjenning av disse fra Utdanningsetaten sentralt. Dersom en ansatt i Osloskolen ønsket å ta i bruk en app som ikke sto i noen av listene over godkjente eller ikke-godkjente tjenester, måtte vedkommende fylle ut et skjema for at tjenesten skulle bli vurdert, og tjenesten skulle ikke tas i bruk før den var godkjent.

På de undersøkte skolene hadde ikke elevene anledning til å selv installere programmer på egen PC. På Nordseter skole hadde alle lærerne administrasjonsrettigheter til egen PC, slik at de kunne installere og teste ut andre programmer og apper enn dem som var godkjent for bruk. På tilsvarende måte hadde lærerne, men ikke elevene, anledning til å logge på App Store med sin personlige Apple-ID, slik at de kunne installere og teste ut ikke-godkjente apper. På Hauketo skole hadde noen lærere administrasjonsrettigheter til egen PC. Ifølge skolen gjaldt dette lærere som hadde særskilt behov for andre programmer og nettjenester enn dem som var godkjent. Lærernes administrasjonsrettigheter til egen PC ga ikke mulighet for å installere ikke-godkjente programmer på elevenes PC-er.

3.2.2 Hauketo skole

Hauketo skole hadde ikke utarbeidet egne oversikter over skolens behandling av personopplysninger. Rektor pekte på at han hadde sett på blant annet behandlingsoversikter og personvernvurderinger utarbeidet av Utdanningsetaten som skolen innhentet våren 2022.

Hauketo hadde ikke gjort særskilte risikovurderinger knyttet til ivaretakelse av personvern. Dette innebar at skolen ikke hadde risikovurdert sine virksomhetsprosesser og bruk av IKT-systemer som innebar behandling av elevenes personopplysninger.

Et eksempel på en slik virksomhetsprosess er utarbeidingen av individuelle opplæringsplaner og årsrapporter for elever med slike planer, jf. kapittel 4. Skolen har oversendt dokumentasjon til Kommunerevisjonen fra andre typer prosesser der det finnes eksempler på vurderinger av forhold knyttet til elevenes personvern. Ett eksempel på dette er en handlingsplan etter vernerunde om fysisk og kjemisk arbeidsmiljø, datert i april 2022, der det framkom at samtaler på lærernes arbeidsrom kunne høres av elever.

Det var Oslobygg KF som var utførende for å få lukket avviket, og avviket ble ifølge rektor lukket innen fristen 20. august 2022. Et annet eksempel er skolens beredskapsplan fra august 2022, der det pekes på at skoleledelsen i en beredskapssituasjon skal sørge for at elevenes personvern beskyttes med tanke på filming og fotografering. I 2013 vurderte skolen den fysiske sikkerheten til arkivrommet med omtale av gjennomførte tiltak.

Ifølge skoleledelsen kunne lærere ha tatt i bruk andre apper enn dem som var godkjent av Utdanningsetatens sentralt, og det var risiko for at lærere tok i bruk nettjenester som behandlet personopplysninger. Ifølge ledelsen skulle lærerne som ønsket å bruke et verktøy, en app eller lignende, bruke det som var godkjent av Utdanningsetaten sentralt. Lærerne hadde ikke fått beskjed om at de ikke skulle bruke andre verktøy, apper og lignende. IKT-ansvarlig oppga at han hadde oversikt over hvilke programmer som var gjort tilgjengelig for brukerne. Han pekte på at enkelte apper likevel kunne installeres uten administratorrettigheter. Det var ikke tilrettelagt for å kontrollere dette.

Kommunerevisjonen snakket med elever som opplyste om at det var vanlig å bruke nettjenester som ikke var godkjent, men at elevene da logget inn via nettleser med sin private bruker. De var ikke kjent med at slike tjenester ble benyttet i undervisningen. Eksempler på slike tjenester var Instagram (bildedelingstjeneste), Snapchat (deling av meldinger, bilder og video), Pinterest (visuell søkemotor) og Messenger (kommunikasjon).

Kameraovervåking

Hauketo skole hadde kameraovervåking. Ifølge rektor hadde skolen hatt dette siden 2015, og i 2019–2020 gjennomførte skolen en prosess med å videreføre kameraovervåkingen. Ifølge skolens søknad til Utdanningsetaten var formålet med kameraovervåkingen å forhindre branntilløp og hærverk og å forebygge kriminell virksomhet knyttet til omsetning og bruk av narkotika, innbrudd og tyveri på skolen. Søknaden gjaldt kameraovervåking utendørs etter alminnelig skoletid. Skolen opplyste at kameraene ble slått på samtidig med skolens innbruddsalarm og følgelig kun var påslått kveld og natt.

Ifølge brev fra Utdanningsetaten til personvernombudet i Oslo, 8. februar 2022, var det Oslobygg KF som hadde driftsansvaret for kameraovervåkingen, og utlevering av opptak ble administrert av foretaket. Skolen presiserte at den ikke hadde tilgang til bilder fra kameraovervåkingen. Skolen hadde ikke søkt om videreføring av kameraovervåkingen i 2021 eller 2022. Våren 2022 utarbeidet skolen rutiner for kameraovervåking, herunder at skolen skulle søke om videreføring av kameraovervåking.

Bruk av e-poster til informasjon av sensitiv karakter

Ifølge skoleledelsen visste de ansatte trolig at de ikke kan bruke e-posten til elevsensitiv informasjon, men de ansatte ville kanskje være usikre på hvor grensen går mellom hva som kan og ikke kan sendes per e-post. Dette var ikke formidlet tydelig fra skolens ledelse til de ansatte. Skoleledelsen oppga at skolen hadde formidlet at den i så stor grad som mulig ønsket å anonymisere e-poster, for eksempel at bruk av initialer ikke var godt nok.

Ansatte kunne innimellom få sensitive opplysninger om elever i e-post fra foresatte, for eksempel helseopplysninger. Rektor trodde at lærerne ikke svarte på slike e-poster uten å slette tråden med sensitivt innhold, men det kunne tenkes at slike e-poster i noen tilfeller ble videresendt internt på skolen. Han oppfattet at det var forskjell de ansatte imellom når det gjaldt i hvilken grad de var bevisste på denne problematikken. Dersom en ansatt fikk en e-post med sensitivt innhold, skulle e-posten legges i elevmappa, for deretter å slettes.

De ansatte vi snakket med, var innforstått med at e-poster med sensitivt innhold ikke skulle videresendes. Det oppsto likevel situasjoner som gjorde at e-poster ble brukt til å sende sensitive opplysninger om elever. For eksempel kunne det skje at foreldre sendte e-poster med sensitive opplysninger. En ansatt oppga å ikke slette tråden med informasjonen, selv om vedkommende visste at hen skulle gjøre det. Videre oppga en ansatt at eventuelle e-poster som kom til kontoret, også de med sensitivt innhold, ble videresendt til aktuelle mottakere. Dersom en legeerklæring ble levert til skolen på papir, måtte den inn i elevens elevmappe. Dette ble løst ved at legeerklæringen ble skannet og overført fra e-post til sikker sone. Det ble pekt på at dette var et dilemma – dokumenter med sensitive opplysninger gikk via e-post til sikker sone. En ansatt oppga å lagre e-poster med sensitivt innhold passordbeskyttet i en mappe på harddisken på PC-en. En ansatt opplyste også at hen pleide å få tilsendt referater fra teammøter per e-post. Enkeltelever ble i slike referater omtalt ved bruk av initialer og informasjon om trinn.

Skolen hadde en «ukeplanlegger» som blant annet inneholdt skolens strategiske plan, oversikt over personalet, ansvar og oppgaver og diverse prosedyrer. I denne framkom det blant annet at norsklærer innen en frist skulle sende en liste til kontoret over hvilke elever som burde få særskilt språkopplæring, og at denne lista skulle sendes på e-post.

Det ble også vist til at det kunne skje at foresatte skrev inn sensitive opplysninger i Skolemeldingsappen, selv om det var spesifisert at det ikke skulle gjøres.

3.2.3 Nordseter skole

Nordseter skole hadde ikke utarbeidet egne oversikter over skolens behandling av personopplysninger. Skolen hadde ikke risikovurdert sine virksomhetsprosesser og bruk av IKT-systemer som innebar behandling av elevenes personopplysninger. Et eksempel på en slik virksomhetsprosess er utarbeidingen av individuelle opplæringsplaner og årsrapporter for elever med slike planer, jf. kapittel 4. Skolen hadde heller ikke vurdert personvernkonsekvenser for denne prosessen.

Når det gjaldt overordnede risikovurderinger, oppfattet skoleledelsen at skolen ved å være underlagt Utdanningsetaten var i et system der alle IKT-systemene som ble brukt, allerede var kvalitetssikret av etaten ved innkjøp/godkjenning. Skolen opplyste at den var klar over at den skulle følge opp elevers og ansattes praksis for å ivareta regler for behandling av personopplysninger (se også kapittel 5.2.3. om opplæring). Skoleledelsen oppga videre at ivaretakelse av personvern var integrert i øvrige prosesser. Skolen har oversendt sin beredskapsplan for vold og trusler mot ansatte på skolen for ungdomstrinnet (revidert 7. desember 2020). Der framkom det blant annet at ledelsen ved skolen ved informasjon om hendelser til personalet og foresatte må vurdere behovet for informasjon opp mot personvernet til involverte lærer(e) og elev(er).

Ifølge skoleledelsen hadde ikke skolen tatt i bruk IKT-systemer som ikke var godkjent av Utdanningsetaten. Skoleledelsen oppga at føringen fra dem var at kun apper og systemer som var godkjent av Utdanningsetaten sentralt, skulle benyttes. Føringen var gitt muntlig, men de mente at det var så tett samarbeid mellom de ansatte på skolen at det trolig ville oppdages raskt dersom en ansatt benyttet andre programmer, systemer og apper enn dem som kunne benyttes. Ledelsen pekte på at skolen hadde et eget ansvar når det gjaldt å ta i bruk apper, nettsider og lignende. IKT-ansvarlig ved skolen gjorde vurderinger om å ta i bruk apper og lignende, og ifølge ledelsen resulterte vurderingene til IKT-ansvarlig noen ganger i at han sa nei til installasjon og bruk. IKT-ansvarlig opplyste at lærere som ville prøve ut apper som ikke var godkjent eller i tråd med kriterier for dette, for eksempel ved at de krevde egen innlogging (ikke gjennom Feide), ikke kunne la elevene ta i bruk tjenesten, og at de ble informert av IKT-ansvarlig om hva som var den personvernmessige utfordringen med den aktuelle tjenesten.

Kommunerevisjonen fikk oversendt informasjon som de ansatte hadde fått fra skolen, knyttet til ulike eksterne innloggingstjenester. Om eksterne innloggingstjenester generelt framgikk det blant annet at Osloskolen ikke hadde databehandleravtale med noen av disse, og at de ansatte selv måtte vurdere om de ville registrere seg med e-postadresse for å opprette konto. Det framkom videre at ansatte ikke hadde lov til å be elever om å registrere sin e-postadresse for å lage kontoer på noen av tjenestene.

Tjenester som var nevnt konkret, var blant annet Mentimeter, Duolingo, Kahoot, Quizlet og Pinterest. For Kahoot og DuoLingo framkom denne informasjonen også i Utdanningsetatens retningslinjer på informasjonssidene for de enkelte tjenestene. For Mentimeter (tjeneste som kan brukes til meningsmåling, avstemninger og undersøkelser) framgikk det på Utdanningsetatens informasjonsside om tjenesten at den behandlet registrerte opplysninger i USA og delte disse med sine underleverandører. Det framgikk videre at kun lærere skulle lage undersøkelser, men at de ikke kunne pålegges å bruke denne tjenesten, og at elever kun skulle delta anonymt ved bruk av engangskode. IPad-appen Quizlet Flashcards & Homework (tjeneste hvor elevene kan lage interaktive spørrekort som kan brukes til øving av ulike fag) er oppført på Utdanningsetatens liste over iPad-apper som er vurdert til «Ikke godkjent for bruk i Osloskolen.» Webtjenesten Quizlet Live var verken oppført på lista over ikke-godkjente eller godkjente webtjenester. Ved Nordseter skole var det distribuert informasjon til lærerne om at elever kunne delta uten egen konto på Quizlets nettsider, men at læreren i så fall måtte opprette konto, enten på nettsidene eller i appen.

Kommunerevisjonen snakket med elever som oppga Pinterest (visuell søkemotor) og Quizlet Live som innloggede nettjenester som ikke var godkjent, men som elever hadde benyttet med sin private bruker og benyttet i skolearbeidet. De var ikke var kjent med at elever var blitt bedt av lærer om å benytte slike tjenester.

Det var ved skolen også gitt informasjon om og retningslinjer for Showbie, herunder om hvordan man skulle opprette en egen bruker, at man måtte velge Feide-innlogging, og hvordan man skulle opprette foreldrekonto. En ansatt ved skolen oppga også at hen mente det var fort gjort å sende invitasjon til feil foresatt, slik at denne kunne få tilgang til personopplysninger om feil barn. Den ansatte oppga å ha nevnt dette i et møte med Utdanningsetatens personverngruppe. Denne risikoen var også poengtert i skolens informasjon til ansatte, nevnt ovenfor.

Bruk av e-poster til informasjon av sensitiv karakter
Ledelsen oppfattet at lærerne generelt var ganske bevisste på ivaretakelse av personvern. De oppga at skolen hadde praksis for å forsøke å anonymisere interne e-poster ved å utelate elevens navn eller ved å bruke elevens initialer, jf. ovenfor. Ledelsen oppga at skolen var innforstått med at dette ikke var optimalt, og at flere lærere var frustrerte over praksisen, men skolen gjorde det slik likevel av praktiske hensyn. Dette gjaldt kommunikasjon mellom lærere, rådgivere og ledelsen som gikk på e-post om enkeltelever – og som kunne omhandle forhold som diagnoser, atferd mv.

Det varierte litt mellom de ansatte vi snakket med, i hvilken grad de oppga å sende sensitive opplysninger per e-post. Vi fikk opplyst at foreldre kunne sende e-poster der de fortalte om hendelser som omfattet en elev, inkludert sensitive opplysninger som medisinbruk, navn e.l. Lærerne oppga at de ikke besvarte slike e-poster uten å slette tråden med de sensitive opplysningene. Dette hadde de fått beskjed om fra ledelsen. Det kunne imidlertid være vanskelig å vite hvor grensen går mellom hvilke opplysninger som kan og ikke kan stå i en e-post. En ansatt oppga også at man ved bruk av e-post skulle bruke initialer på elevene, og at vedkommende gjorde det. Det ble også pekt på at viktige e-poster måtte arkiveres, og måtte videresendes til rådgiver for overføring til Websak.

3.3 Kommunerevisjonens vurderinger

De undersøkte skolene hadde i noen grad oversikt over sin behandling av elevenes personopplysninger i administrative systemer og i apper og nettjenester som skolene benyttet i undervisningen, gjennom dokumentasjon som Utdanningsetaten sentralt hadde utarbeidet. Videre hadde Utdanningsetaten sentralt gjennomført enkelte personvernkonsekvensvurderinger og en rekke risikoanalyser, herunder for det skoleadministrative systemet IST Everyday og for læringsteknologiske apper og tjenester.

Utdanningsetaten hadde ikke ferdigstilt personvernkonsekvensvurderinger for læringsteknologien som var i bruk i Osloskolen. Kommunerevisjonen merker seg at etaten arbeidet med dette. Det var en mangel at IST Everyday ble tatt i bruk før personvernkonsekvensvurderingen var gjennomført.

Ingen av de undersøkte skolene hadde gjort vurderinger av om oversiktene som var utarbeidet, var dekkende for skolens bruk av ulike systemer og digitale tjenester og for behandling av elevers personopplysninger i disse. Dette ga risiko for at det ble behandlet personopplysninger i systemer og verktøy ved skolene som ikke var omfattet av Utdanningsetatens vurderinger.

Skolene hadde heller ikke dokumentert vurderinger av om det var risikoer forbundet med måten skolene benyttet systemene, herunder av hvordan skolen gjennomførte virksomhetsprosesser som involverte behandling av elevers personopplysninger. For eksempel hadde begge skolene prosesser for utarbeiding av individuelle opplæringsplaner og årsrapporter for elever med slike planer, som omfattet særlige kategorier personopplysninger. Skolene hadde ikke gjennomført personvernkonsekvensvurderinger for disse prosessene. Disse dokumentene ble behandlet i systemer som ikke var godkjent for slike personopplysninger. Det var også risiko for at skolene behandlet sensitive elevopplysninger i e-post, noe som forekom ved begge skolene. Kommunerevisjonen merker seg at Utdanningsetaten var kjent med at

skolene manglet et verktøy for samhandling mellom ledelse og lærere for behandling av særlige kategorier personopplysninger. Etaten oppga at den hadde igangsatt et langsiktig arbeid med anskaffelse av et slikt verktøy.

Nordseter skole og andre skoler som brukte iPad, benyttet Showbie, der elevers personopplysninger ble behandlet. Kommunerevisjonen stiller spørsmål ved at etaten ikke hadde gjennomført en fullstendig personvernkonsekvensvurdering av systemet, ettersom systemet inneholder læreres vurdering av elevarbeider.

4. Tilgangsstyring

4.1 Revisjonskriterier

Kommunerevisjonen har lagt følgende revisjonskriterier til grunn:

- Skolen skal ha oversikt over hvem som har tilgang til personopplysninger om elever, både materielt og i IT-systemer.
- Tilgang til personopplysninger om elever skal være i samsvar med tjenstlig behov.

Kommunerevisjonen har lagt til grunn at det skal være etablert rutiner og praksis for en tilfredsstillende tilgangsstyring i de utvalgte systemene. Rutiner for tilfredsstillende tilgangsstyring bør omfatte blant annet tildeling, endring og gjennomgang av tilganger.

4.2 Faktabeskrivelse

4.2.1 Fakta som gjelder alle – Utdanningsetatens system

Utdanningsetaten hadde en instruks for tilgangsstyring der det blant annet framkom at «[l]edere på alle nivåer er ansvarlig for å sikre at sine ansattes tilganger og rettigheter kun gis basert på tjenstlig behov, korrigeres ved endringer og fjernes ved opphør av ansettelsesforhold».

Etaten hadde også en egen sikkerhetsinstruks for ansatte i skolene. Ifølge instruksen skulle denne være lest og signert av alle ansatte ved oppstart i stilling og deretter ved årlig medarbeidersamtale. Instruksen inneholdt blant annet informasjon om behandling av informasjon, deriblant at ledere er ansvarlig for å gi tilganger etter prinsippet om tilgang i henhold til tjenstlig behov, og at fortrolig informasjon ikke skal skrives i fritekstfelt eller kommentarfelt i fagsystemer. Videre het det at den ansatte skulle gjennomgå generell opplæring i informasjonssikkerhet og personvern før vedkommende får tilgang til de aktuelle IKT-systemene.

4.2.2 Hauketo skole

Tilgangsstyring til personopplysninger som er lagret digitalt

Når nye lærere startet ved skolen, ble de av kontoret registrert inn i HR-systemet og gitt tilganger i det skoleadministrative systemet IST Everyday basert på informasjon fra skoleledelsen om hvilken rolle den ansatte skulle ha. Informasjonen om den ansattes rolle ble importert til Driftsportalen og ga de ansatte tilganger til andre systemer i Skoleplattform Oslo, som Itslearning, Teams, Skolemelding mv. Hvilke opplysninger en ansatt hadde tilgang til, var avhengig av vedkommendes rolle i systemet. Eksempelvis hadde faglærere kun tilgang til informasjon i IST Everyday om fravær og karakterer i egne fag, mens kontaktlærere hadde tilgang til alle fraværs- og karakteropplysninger om egne elever. Videre ga tilgangen i IST Everyday tilgang til administrerte Teamsgrupper, herunder for de enkelte klassetrinn.

Rektor oppga at han bestilte tilganger til ansatte i skolens administrasjon ved hjelp av et eget skjema på Utdanningsetatens intranett, Tavla. Når det gjaldt lærerne, var det rektor som formelt besluttet hvem som skulle ha hvilke tilganger, gjennom en stillingsplan som ble utarbeidet i forkant av hvert skoleår. Stillingsplanen inneholdt informasjon om hvilke lærere som underviste i hvilke fag og klasser, samt hvem som var kontaktlærer i hvilken klasse. Skoleledelsen vurderte risikoen for at det ble gjort endringer i planen slik at uvedkommende fikk tilgang til opplysninger uten tjenstlig behov, som liten. Ifølge

skoleledelsen ble planen gjennomgått og sjekket gjentatte ganger av ledelsen. Den lå også lagret på et filområde som kun administrasjonen hadde tilgang til. Stillingsplanen ble sendt til alle ansatte i PDF-format. Stillingsplanen styrte timeplanen, og hvis det ble oppdaget feil i oppsettet, ble feilen rettet.

Det ble ikke gjennomført kontroller i løpet av skoleåret av om tilgangene var riktige, men det ble ifølge ledelsen fort oppdaget hvis noen hadde tilganger de ikke skulle ha. Ifølge ledelsen var det en utfordring å slette tilganger hvis en lærer sluttet eller fikk en annen rolle. Det var ikke rutine for å stoppe tilganger underveis i skoleår. Tilgangene ble imidlertid gjennomgått årlig på vårparten, når man gjorde klar tilgangene til nytt skoleår. Da ble alle tilganger og roller lagt inn på nytt.

Deling av elevinformasjon mellom administrasjon og lærerne

Elevmapper ble arkivert i Websak. Det var kun administrasjonen, det vil si ledelsen, de ansatte på kontoret og rådgiverne, som hadde tilgang til Websak, mens lærerne ikke hadde det. Rektor oppga at det var han som bestilte tilganger i Websak. Ifølge rektor inneholdt elevmappene blant annet informasjon fra elevenes barneskole som den aktuelle barneskolen hadde vurdert at kontaktlæreren på ungdomsskolen hadde behov for. Rektor vurderte at lærerne på skolen hadde tjenstlig behov for disse opplysningene, og at denne ordningen derfor ikke fungerte godt i praksis. For å ivareta lærernes informasjonsbehov hadde rådgiver, ifølge rektor, overføringsmøter med den enkelte kontaktlærer ved oppstarten av et nytt skoleår, der rådgiver videreformidlet informasjon om elevene til den enkelte kontaktlærer. Dersom en lærer senere hadde behov for informasjon fra en elevmappe, skulle vedkommende ta kontakt med rådgiver, som kunne skrive ut aktuell informasjon fra elevmapper. Utskriften skulle så makuleres.

Ifølge skoleledelsen ble deling av sensitive opplysninger som regel gjort muntlig i møter. Dersom informasjonen ble skrevet ned, ble den ifølge dem lagret i Websak. Referater fra «elevmøter» i skolemiljøsaker ble ifølge ledelsen lagret i et eget filområde på «sikker sone» i Websak. Det ville si at kun deltakerne i møtet skulle ha tilgang. Ledelsen vurderte at informasjonen var godt nok sikret. Skoleledelsen oppga at det våren 2022 hadde kommet nye rutiner for varsling i skolemiljøsaker. Etter dette skulle varsler sendes direkte i Websak, via lenker i Skoleplattform Oslo, mens varsler tidligere ble sendt per e-post.

Dokumentasjon knyttet til spesialundervisning, blant annet individuelle opplæringsplaner, sakkyndige vurderinger fra PPT (Pedagogisk-psykologisk tjeneste), vedtak om spesialundervisning og årsrapporter lå lagret i sikker sone i Websak. I tillegg ble de individuelle opplæringsplanene og årsrapportene lagret på et eget område i SharePoint for at lærerne skulle ha tilgang til dokumentene. Alle lærerne hadde tilgang til alle disse dokumentene. Dokumentene skulle være anonymiserte, men det var de ikke alltid. Vi fikk opplyst at enkelte brukte elevens initialer, andre brukte navn i dokumentene, mens noen ganger sto navnefeltet tomt. Vi åpnet en tilfeldig individuell opplæringsplan, og der framgikk elevens fulle navn. Vi fikk opplyst at årsrapporter og pedagogiske rapporter (i forkant av et vedtak) for alle elevene som i løpet av fjoråret enten fikk en individuell opplæringsplan eller ble utredet for dysleksi, også lå i SharePoint-løsningen.

Individuell opplæringsplaner og årsrapporter ble produsert av lærerne, men de kunne ikke gjøre dette arbeidet i Websak, ettersom de ikke hadde tilgang til systemet. For at

lærerne skulle få tilgang til de aktuelle sakkyndige vurderingene i arbeidet, ble dokumentene skrevet ut og oppbevart i permer for hvert klassetrinn i skap på lærernes arbeidsrom. Når det gjaldt hvordan dokumentene ble lagret underveis i arbeidet, fikk vi ulike opplysninger om hvordan de ansatte løste dette i praksis. En oppga å lagre de individuelle opplæringsplanene i sine personlige lagringsområder i Office 365, mens en annen oppga å redigere dokumentet i SharePoint.

Vi fikk opplyst at det var et eget punkt på agendaen i teammøter der lærerne kunne ta opp forhold, bekymringer o.l. knyttet til enkeltelever. Referatene fra disse møtene var tilgjengelig for alle lærerne i SharePoint. I referatene skulle konkrete elever omtales med initialer og klassetilhørighet. Det ble pekt på at lærere kunne ha behov for tilgang til alle referatene dersom de var inne i undervisningen i mange klasser. Samtidig ble det pekt på at bruk av initialer og klassetilhørighet ikke var tilfredsstillende anonymisering.

Skoleledelsen oppga at skolen ikke hadde tydelige rutiner for behandling av elevdata, og at det nok følgelig var variasjon i praksis.

Som beskrevet i kapittel 3.2.2. avdekket skolen i april 2022 at samtaler på lærernes arbeidsrom kunne høres av elever, og sikret at det ble gjennomført risikoreduserende tiltak innen starten på neste skoleår.

I kommunikasjon med foreldre ble også telefonsamtaler brukt. Det ble pekt på at det kunne være en utfordring å finne et privat sted å ta slike samtaler, og at ansatte gjerne måtte snakke i telefonen mens kollegaer var til stede og kunne høre samtalen.

Adgangskontroll til fysisk arkiv

Skolen hadde en skriftlig rutine for adgang til arkivrom og arkivdepot (udatert), der det framkom at det var montert adgangskontroll på dørene til arkivrommet og arkivdepotet for å begrense adgangen til disse rommene. Adgang til arkivrom var forbeholdt ansatte i administrasjonen. Adgang til arkivdepotet var gitt kun til ansatte med behov for det.

Vi fikk opplyst at elevmapper ble oppbevart i to ulike fysiske arkiver: et fjernarkiv (med gamle elevmapper) og et arkivskap i administrasjonen (med nyere elevmapper, fram til overgangen til Websak i mars 2019). Arkivskapet ble låst med en nøkkel som ble oppbevart på kontoret. Rommet der arkivskapet sto, var låst, og ansatte med adgang måtte bruke nøkkelkortet sitt for å komme inn. Vi fikk opplyst at dette gjaldt ledelsen, de ansatte på kontoret og rådgiverne, i tillegg til kanskje noe driftspersonell. Lærere hadde ikke tilgang.

Dersom en lærer hadde behov for tilgang til informasjon i arkivskapet, skulle vedkommende henvende seg til kontoret, og en av de ansatte ved kontoret skulle låse opp. Det var ikke så ofte at lærerne hadde behov for tilgang på dokumentasjon som lå lagret i arkivskapet. Når det skjedde, fant en ansatt på kontoret den konkrete elevmappa og ga til læreren. Vedkommende skulle sitte på kontoret og lese informasjonen.

Bruk av notatbøker o.l.

Det var ikke gitt noen føringer fra skoleledelsen når det gjaldt hvor lærerne skulle notere seg opplysninger om elevene, observasjoner i undervisningen mv. Skoleledelsen så det som nødvendig at Utdanningsetaten sentralt ga føringer om slike forhold. Det varierte de ansatte imellom hvor de noterte seg slike opplysninger. Metodene som ble benyttet, var

en skriftlig oversikt i den ansattes eget lagringsområde i Office 365 og fysiske notater (i notatbok eller på papirskjema). Notatene ble oppbevart innelåst på arbeidsrom. Én lærer oppga at notater ble låst inn i en skuff. Det varierte om andre hadde tilgang til arbeidsrommene. Det ble også nevnt at notater på papir ble overført til sikker sone ved hjelp av skanning og oversending via e-post.

4.2.3 Nordseter skole

Tilgangsstyring til personopplysninger som er lagret digitalt

Tilganger ble ved begynnelsen av hvert skoleår opprettet på nytt for alle ansatte, på bakgrunn av en oversikt som kontoret fikk av rektor. Oversikten inneholdt informasjon om alle klassene og alle fagene som klassene har, samt lærerne som var tilknyttet hver klasses fag.

Informasjonen om den ansattes rolle ble importert til Driftsportalen (verktøy der skolenes IKT-ansvarlige administrerer brukere, programvare og maskiner), og dette ga de ansatte tilganger til andre systemer i Skoleplattform Oslo, som Itslearning, Teams, OneNote, Skolemelding mv. Hvilke opplysninger en ansatt hadde tilgang til, var avhengig av vedkommendes rolle i systemet. Eksempelvis hadde faglærere kun tilgang til informasjon i IST Everyday om fravær og karakterer i egne fag, mens kontaktlærere hadde tilgang til alle fraværs- og karakteropplysninger om egne elever. Videre ga tilgangen i IST Everyday tilgang til administrerte notatblokker i OneNote, herunder for de enkelte klassetrinn og klasser.

Når det gjaldt tilganger for ledere og administrasjonen, fikk vi oppgitt at rektor bestilte tilganger til de aktuelle ansatte, herunder til Websak, og avgjorde om den ansatte skulle ha tilgang til sikker sone.

Skolen oppga at ledelsen og kontoret kommuniserte løpende om endringer av tilganger, herunder ved nyansettelser, endringer og avslutning av stillinger. Kontoret på Nordseter skole registrerte ifølge kontorleder nyansatte i HR-systemet og i det skoleadministrative systemet IST Everyday etter informasjon fra rektor om hvilke klasser og fag læreren skulle ha det aktuelle skoleåret. Ledelsen oppga at den ikke var involvert i kontroller av tilganger underveis i et skoleår, kun i den årlige gjennomgangen. Ledelsens erfaring var at kontoret normalt fanget opp og avsluttet tilganger dersom noen ansatte sluttet i løpet av et skoleår. Dersom slike endringer ikke ble fanget opp, ble alle tilgangene endret eller avsluttet i den årlige gjennomgangen. Ifølge kontoret hadde alle midlertidig ansatte en avslutningsdato i systemet, og tilgangene ble avsluttet på den registrerte sluttdatoen. Dersom en ansatt lærer overtok en eller flere elever for en periode, ville vedkommende ofte ha tilgangen ut skoleåret.

Deling av elevinformasjon mellom administrasjon og lærerne

Ledelsen oppga at dersom en lærer ønsket å drøfte forhold ved en elev med skolens ledelse, skulle læreren gi beskjed til ledelsen om dette per e-post, og så tok læreren og ledelsen en prat. Når slike beskjeder ble gitt per e-post, ble eleven benevnt med initialer eller «den eleven», navn ble ifølge dem ikke brukt. Ansatte bekreftet å ha fått beskjed om at sensitive opplysninger ikke skulle stå der navnet på den som opplysningene gjelder, framgår.

Som nevnt tidligere, lå elevmappene i Websak. Følgelig var en rekke dokumenter knyttet til enkeltelever arkivert der. Lærerne på skolen hadde ikke tilgang til sikker sone og

Websak. Skoleledelsen opplevde dette som en utfordring. De oppga at det per i dag ikke fantes en teknisk løsning som var godkjent for lagring av sensitive opplysninger, og som muliggjorde kommunikasjon på tvers på skolen. Skolen oppga at både ledelsen ved skolen og IKT-ansvarlig hadde etterspurt dette fra Utdanningsetaten. At lærerne ikke hadde tilgang til Websak, medførte for eksempel at lærerne ikke har tilgang til aktivitetsplaner i skolemiljøsaker. Tidligere var aktivitetsplanene tilgjengelig i fysisk format. Også referater fra møter i skolemiljøsaker ble lagret i Websak. Dersom en lærer hadde behov for å lese dokumentasjon i slike saker, skulle vedkommende henvende seg til en ansatt med tilgang og få lese dokumenter på dennes skjerm eller få en utskrift av den aktuelle dokumentasjonen.

Lærernes manglende tilgang til Websak utgjorde også ifølge skolen en utfordring når det gjaldt deling av og arbeid med dokumentasjon knyttet til spesialundervisning. Skolens praktiske løsning for dette var å lagre individuelle opplæringsplaner og årsrapporter i SharePoint. Dokumentene ble ikke kryptert, men elevene ble forsøkt anonymisert ved at initialene deres ble benyttet i dokumentene. Alle ansatte som underviste fast ved skolen, hadde tilgang til alle de individuelle opplæringsplanene og årsrapportene. Om de omtalte elevene var identifiserbare, var avhengig av hvem som leste, og hvor tett læreren var på de aktuelle elevene. Skolen var innforstått med at dette ikke var en god løsning, men opplevde det som den eneste praktiske måten å løse dette på. Det ble pekt på at det var en grenseoppgang å sikre at alle som hadde tjenstlig behov, hadde tilgang, uten å risikere at informasjonen kom på avveie. Skolen opplyste primo september om at den hadde gjennomført tiltak for å begrense lærernes tilgang til individuelle opplæringsplaner og årsrapporter, slik at kun lærere på ungdomstrinnet hadde tilgang til dokumentene for ungdomsskoleelever og kun lærere på barnetrinnet hadde tilgang til dokumentene for elever på barnetrinnet.

For at lærerne skulle få tilgang til de aktuelle sakkyndige vurderingene i arbeidet med individuelle opplæringsplaner, opplyste skolen at lærerne fikk utskrifter av dokumentene, og at de oppbevarte disse i en skuff på arbeidsrommet sitt. Arbeidsrommene ble delt av flere lærere, og alle lærere hadde adgang ved bruk av nøkkel. Kommunerevisjonen fikk opplyst at det varierte om lærerne oppbevarte dokumentene i låst skuff på arbeidsrommene, og om de hadde skuff det var mulig å låse. Underveis i arbeidet med de individuelle opplæringsplanene ble disse lagret i lærerens OneDrive.

Forhold knyttet til enkeltelever ble også diskutert i teammøter. Vi fikk opplyst at teammøtene ikke ble referatført, men at det kunne bli utarbeidet enkle notater, uten opplysninger om navn på elever – disse ble kun nevnt i selve møtet. Det varierte litt blant de ansatte når det gjaldt opplevd bevissthet rundt at disse møtene skulle holdes private. En ansatt erfarte at håndtering av muntlig informasjon ikke alltid ble håndtert på en god måte, og hen oppga for eksempel at det hendte at teammøter og omtale av elever foregikk steder det ikke burde foregått, for eksempel der det var andre ansatte til stede. En annen ansatt oppga at hen opplevde at det var bevissthet knyttet til hvem som var til stede, og til at døra til rommet måtte være lukket. Også i andre sammenhenger ble informasjon tatt opp muntlig. Lærerne oppga at de ringte til foresatte dersom de hadde behov for å ta opp noe knyttet til en elev. I den forbindelse ble det pekt på at det kunne være en utfordring å finne et privat sted å ta slike samtaler, og at man gjerne måtte snakke i telefonen mens kollegaer var til stede og kunne høre samtalen.

Nordseter skole benyttet også OneNote til ulike formål. Blant annet ble klassenotatblokkene benyttet. Dette var i løpet av siste året tatt i bruk i stedet for Showbie på ungdomstrinnet. Vi fikk opplyst at klassenotatblokkene og tilgangen til disse ble opprettet via driftsportalen. I disse notatblokkene ble det lagt ut ressurser til elevene i tillegg til at det var samarbeidssider, og hver elev hadde sin egen side som kun eleven selv og læreren hadde tilgang til.

Vi fikk opplyst at det var laget en struktur for OneNote og inndeling i grupper etter samarbeidsbehov. Dette var gjort for at det ikke skulle være fritt fram å opprette OneNote-notatblokker til egne formål. Når det gjaldt samarbeid mellom lærere, var det blant annet egne inndelinger for ulike fag og trinn. Det var også en egen inndeling for team (to klasser), der tre kontaktlærere hadde tilgang til en passordbeskyttet inndeling for «Elevene». Der kunne lærerne notere seg nødvendig informasjon fra utviklingssamtaler, elevsamtaler, møter med eksterne etc. Referater fra møter med eksterne aktører ble lagret i Websak. Det ble pekt på at det var en risiko for at noen skrev inn sensitive opplysninger eller informasjon som ikke andre burde se, og at skolen for å redusere denne faren hadde gitt færrest mulig tilgang og passordbeskyttet inndelingen. Vi fikk også opplyst at skolen hadde gitt beskjed til lærerne om at dette ikke var et sted som er ansett som sikkert, slik som Websak, og at de skulle være forsiktig med hva de skrev der. Mer informasjon om hvordan de ansatte noterte seg ting fra timer, utviklingssamtaler og lignende, er nærmere omtalt lenger ned under «Bruk av notatbøker o.l.»

Adgangskontroll til fysisk arkiv

Nordseter skole hadde et fjernarkiv med elevmapper og et arkivskap på kontoret med personalmapper, saksarkiv og noen elevmapper. Skoleledelsen og kontoret opplyste at skolen hadde et nivåbasert nøkkelsystem, der de som var definert på et bestemt nivå, i dette tilfellet ledelsen, rådgiverne og kontoret, hadde tilgang til fjernarkivet og arkivskap. Hvis en lærer hadde behov for tilgang til en elevmappe i fjernarkivet eller arkivskap, skulle vedkommende henvende seg til kontoret som hentet ut den aktuelle dokumentasjonen til læreren. Læreren skulle enten se gjennom dokumentasjonen på kontoret, ev. få en kopi av et brev som skulle makuleres etter gjennomlesing. Dette var ikke nedfelt i en skriftlig rutine.

Bruk av notatbøker o.l.

Det var ikke gitt føringer fra skoleledelsen når det gjaldt hvordan lærerne skulle bruke og oppbevare notater fra timer, møter og lignende. Skoleledelsen oppga at den overfor ansatte hadde pekt på muligheten for å passordbeskytte filer og inndelinger i OneNote. Skolen hadde i den forbindelse ikke lagt føringer for passordstyrke. Vi fikk ulike opplysninger fra lærerne når det gjaldt hvordan de noterte seg ting fra timene, utviklingssamtaler og lignende. Én oppga at hen brukte passordbelagte notater i OneNote til dette formålet. Andre ansatte oppga at de noterte på Post-it-lapper eller i en egen skrivebok til dette formålet. Én ansatt oppga å dokumentere enkelthendelser på sin private mobiltelefon, enten i form av et lydopptak eller notat, sånn at hen husket det. Vedkommende presiserte at slike notater og opptak aldri inneholdt elevnavn, og at opptaket/notatet ble slettet med en gang det var skrevet inn i ei notatbok. Notatbok og Post-it-lapper ble oppbevart enten på arbeidspulten eller i et ulåst skap på de aktuelle lærernes arbeidsrom. Vi fikk opplyst at arbeidsrommene var låst, og at alle ansatte på

skolen kunne låse seg inn med egen nøkkel. Lærerne ønsket at de hadde mulighet til å låse notatbøkene/lappene inn i en skuff eller et skap.

4.3 Kommunerevisjonens vurderinger

Undersøkelsen viser at både Hauketo skole og Nordseter skole hadde rutiner som var egnet til å sikre at skolen hadde oversikt over de ansattes tilganger til informasjon i IST Everyday og andre systemer i Skoleplattform Oslo, som Itslearning, Teams, OneNote, Skolemelding mv. Dette ga også mulighet til å sikre at tilgangene var i samsvar med tjenstlig behov. Ved begge skolene ble tilgangene til disse systemene gitt på bakgrunn av en oversikt over roller som skoleledelsen utarbeidet. Denne praksisen bidro til at skoleledelsen hadde oversikt over hvem som ble gitt ulike tilganger i disse systemene, og at disse tilgangene var i tråd med den ansattes rolle. Ifølge skolene ble disse tilgangene gjennomgått årlig, ved at alle tilgangene ble satt på ny i forbindelse med nytt skoleår, på grunnlag av en ny oversikt fra skoleledelsen. Ved begge skolene var det svakheter i rutinene for å sikre at tilganger ble avsluttet i løpet av et skoleår hvis det tjenstlige behovet falt bort. Undersøkelsen tyder på at begge skolene hadde oversikt over hvem som hadde adgang til fysisk arkiv, der eldre elevmapper ble oppbevart.

Websak er skolenes saks- og arkivsystem og inneholdt blant annet elevmappene. Skolene hadde rutiner som var egnet til å sikre at ingen ansatte fikk tilganger til dette systemet utover sitt tjenstlige behov. Imidlertid hadde ikke lærerne ved noen av skolene tilgang til systemet. Dette ga skolene utfordringer med å sikre lærerne tilstrekkelig tilgang til personopplysninger om elevene og tilgang til et sikkert sted å behandle slike opplysninger digitalt. Dette kan ha bidratt til en praksis ved begge de undersøkte skolene der lærere som ikke hadde tjenstlig behov, hadde tilgang til elevers individuelle opplæringsplaner og årsrapporter for elever med slike planer i et system som ikke var godkjent for behandling av særlige kategorier personopplysninger, jf. delkapittel 3.3.

Forsøk på anonymisering av elever ved bruk av initialer forekom ved begge skolene, blant annet i individuelle opplæringsplaner og årsrapporter. Bruk av initialer ved formidling av informasjon av sensitiv karakter per e-post forekom også ved begge skolene, jf. kapittel 3.2. Kommunerevisjonen mener det er høy risiko for at ansatte uten tjenstlig behov kunne identifisere elevene også når navnet ikke framgikk, og vil peke på at det er risiko for at disse dokumentene kunne inneholde særlige kategorier personopplysninger og andre sensitive opplysninger. For at lærerne skulle ha tilgang til nødvendige dokumenter i forbindelse med arbeid med individuelle opplæringsplaner, fikk lærerne utskrifter av disse. Undersøkelsen tyder på at det kunne variere om disse ble oppbevart på en slik måte at det kun var lærere med tjenstlig behov som hadde adgang.

5. Opplæring og kompetanse

5.1 Revisjonskriterier

Kommunerevisjonen har lagt følgende revisjonskriterium til grunn:

- Skolen skal sørge for at de ansatte ved skolen har tilfredsstillende kompetanse til å kunne ivareta elevenes personvern.

5.2 Faktabeskrivelse

5.2.1 Fakta som gjelder alle – Utdanningsetaten

Utdanningsetaten hadde utarbeidet ulike e-læringskurs om informasjonssikkerhet o.a. – ett som var obligatorisk for alle ansatte i Osloskolen, og ett som var obligatorisk for IKT-ansvarlige.

E-læringskurset som var obligatorisk for alle ansatte i Osloskolen, besto av fem leksjoner, hvorav hver var anslått å ta 10–15 minutter å gjennomføre. Én av leksjonene omhandlet håndtering av personopplysninger. Leksjonen inneholdt informasjon om

- hva en personopplysning er
- hva som regnes som håndtering av personopplysninger
- prinsipper for behandling av personopplysninger
- hva informasjonsverdier er
- hvordan informasjonsverdier behandles
- sensitive personopplysninger

Videre var det eksempler på typiske hendelser som kan oppstå på en skole, der personopplysninger håndteres: «en lærer tar notater i forbindelse med en voldsepisode» og «en lærer mottar en e-post med helseopplysninger fra en foresatt». Det var også beskrevet hvordan slike hendelser skal håndteres. E-læringen omfattet også noen spørsmål knyttet til tematikken som respondenten skulle besvare eller reflektere rundt/tenke gjennom.

Utdanningsetatens e-læringskurs for IKT-ansvarlige omfattet blant annet informasjon om godkjent produktliste, apper, programvare og lisenser, driftsportalen, bruk av Office 365, Teams og OneNote. E-læringen hadde også en modul om informasjonssikkerhet og personvern.

5.2.2 Hauketo skole

Ifølge ledelsen på Hauketo skole gjennomførte ti ansatte i administrasjonen på skolen opplæring i personvern i forbindelse med sikkerhetsmåneden i 2018. Lærerne hadde ikke gjennomført slike opplæringsaktiviteter. Ledelsen oppga våren 2022 at den ikke hadde fått informasjon fra Utdanningsetaten om opplæring i personvern etter 2018, og at det ikke hadde vært gjennomført slik opplæring siden. De oppga videre at personvern ikke hadde vært tema i fellesmøter, avdelingsmøter e.l. ved skolen. Skoleledelsen oppga at opplæringen som ansatte hadde fått i bruk av IKT-verktøy ikke hadde omfattet informasjonssikkerhet og personvern. Tre av de ansatte i administrasjonen oppga at de hadde gjennomført kurs i personvern i løpet av de siste årene, to i form av e-læringskurs.

Det varierte mellom de ansatte om de opplevde å ha god nok kompetanse om ivaretakelse av personvern, og flere pekte på at de opplevde å ha behov for mer

opplæring/kompetanse. Ansatte oppga at det hadde vært en liten bolk med overordnet informasjon om IKT i forbindelse med planleggingsdagene ved starten av skoleåret 2022/2023.

Skoleledelsen opplevde at lærerne hadde god forståelse av taushetsplikten sin, men de trodde at krav knyttet til ivaretakelse av elevenes personvern for øvrig var uklare for lærerne. De vurderte at det var behov for opplæring knyttet til ivaretakelse av elevenes personvern.

5.2.3 Nordseter skole

Ledelsen på Nordseter skole oppga at skolen hadde gjennomført Utdanningsetatens e-læringsopplegg der personvern var omfattet. Ledelsen var noe usikker på når dette sist ble gjennomført, men trodde det var i skoleåret 2019/2020. Det hadde ikke vært gjennomført i skoleåret 2020/2021 eller 2021/2022. Det var også gjennomført e-læringsopplegg høsten 2018 i forbindelse med nytt GDPR-regelverk. Kommunerevisjonen fikk framlagt dokumentasjon som viste at ledelsen hadde sendt påminnelser til de ansatte som etter utsending ikke hadde gjennomført e-læringsopplegget i 2018. Skoleledelsen opplyste at nyere tilsvarende korrespondanse var sendt i portalen som meldinger til de ansatte, men kunne ikke gjenfinne disse. Ifølge ledelsen kunne skolen tidligere gå inn og se hvilke ansatte som hadde gjennomført e-læringskurs, men det var ikke lenger mulig.

Videre oppga ledelsen at skolens ansatte deltok i opplæringsopplegget i forbindelse med sikkerhetsmåneden. Rektor sa at han oppfattet at det var bestemt av Utdanningsetatens administrasjon at skolene skulle delta i dette opplegget. Det varierte mellom de ansatte vi snakket med, om de hadde deltatt i opplegget i forbindelse med sikkerhetsmåneden.

Ledelsen oppga at temaet personvern ut over dette ikke systematisk ble tatt opp med de ansatte på skolen, og ledelsen vurderte at opplæring og tematisering av personvern per nå ikke var godt nok ivaretatt på skolen. Dette hang blant annet sammen med at ledelsen hadde en forventning om at lærerne gjennom utdanningen sin fikk innsikt og ferdigheter i tematikken. Ledelsen oppga imidlertid at temaet fra tid til annen ble tatt opp, gjerne i forbindelse med hendelser der personopplysninger ikke hadde blitt behandlet på riktig måte. Vi fikk opplyst at lærerne fikk informasjon i diverse møter, pedagogisk utviklingstid (PU-tid), plandager, i OneNote og lignende. Skolen oppga blant annet at de ansatte fikk beskjed om hvordan ulike forhold skulle håndteres, eksempelvis bruk av klasselister, om bruk av foto og kommunikasjon på melding (i Portalen), at ved svar på e-poster fra foresatte med personvernsensitiv informasjon skulle de ansatte starte på en ny e-post, og at ansatte ikke skulle be elever om å legge igjen e-postadressen sin på internettsider og lignende. Framlagt dokumentasjon understøtter at temaer knyttet til IKT ble tatt opp på plandagene. Vi fikk også informasjon som viste at ansatte på skolen fikk informasjon knyttet til IKT via OneNote, jf. informasjon i delkapittel 3.2.3.

Som det også framkommer i delkapittel 3.2.3, hadde skolen et område i OneNote med informasjon til de ansatte knyttet til IKT.

Alle de ansatte vi snakket med, oppga at de hadde gjennomført opplæringsaktiviteter som omfattet personvern. Enkelte ansatte pekte i den forbindelse på at tilgjengelig tid var en utfordring når det gjaldt å gjennomføre opplæringen – slike aktiviteter kommer på toppen av alt annet som skal gjøres. Én pekte på at fokus må være at skolen har god

kultur og praksis for ivaretakelse av personvern. Det ble blant annet pekt på at det kunne være vanskelig å vite hva som er personopplysninger, og hvor skillet mellom sensitive og ikke-sensitive personopplysninger går.

5.3 Kommunerevisjonens vurderinger

Skolene hadde tilgang til opplæringsmateriell utarbeidet av Utdanningsetaten som syntes egnet til å styrke personvernkompetansen.

Hauketo skole hadde ikke sikret tilfredsstillende opplæring i personvern for de ansatte ved skolen. Kun enkelte av de ansatte hadde gjennomført opplæringsaktiviteter, og for mange var det flere år siden sist. Flere av dem vi snakket med, opplevde å ha behov for mer opplæring.

Nordseter skole hadde gjennomført opplæringsaktiviteter som kunne styrke de ansattes kompetanse i ivaretakelse av elevenes personvern. Det er vanskelig å fastslå om kompetansen var tilfredsstillende, men Kommunerevisjonen merker seg at ansatte opplevde enkelte utfordringer, som å ha tilstrekkelig tid til å gjennomføre opplæring, og å skille mellom sensitive og ikke-sensitive personopplysninger. Kommunerevisjonen stiller derfor likevel spørsmål ved om opplæringen var tilstrekkelig til sikre alle ansatte tilfredsstillende kompetanse.

6. Avvikshåndtering

6.1 Revisjonskriterier

Kommunerevisjonen har lagt følgende revisjonskriterier til grunn:

- Skolen skal ha rutiner og praksis for å håndtere hendelser og avvik knyttet til informasjonssikkerhetshendelser som rammer personopplysninger om elever.
- Skolens håndtering av hendelser og avvik knyttet til elevers personopplysninger skal være dokumentert.

6.2 Faktabeskrivelse

6.2.1 Fakta som gjelder alle – Utdanningsetaten

Som del av styringssystemet for informasjonssikkerhet og personvern hadde Utdanningsetaten utarbeidet en instruks for avvikshåndtering innen informasjonssikkerhet og personvern, instruks for roller og ansvar og en sikkerhetsinstruks for ansatte i skolen. Som nevnt lå styringssystemet tilgjengelig på intranettet Tavla. I instruks for roller og ansvar framgikk det blant annet at rektor hadde operativt ansvar for å sikre at alle avvik innen informasjonssikkerhet og personvern ble rapportert til Utdanningsetaten. Instruksen for avvikshåndtering beskrev blant annet hva et avvik innen informasjonssikkerhet og personvern er, samt hvordan og til hvem avvik skal rapporteres. Det framgikk også av instruksen at alle ansatte hadde plikt til å melde mulige eller observerte avvik så snart som mulig. Av sikkerhetsinstruksen for ansatte i skolen framgikk det at alle avvik som hovedregel skulle meldes til nærmeste leder, som skulle rapportere avvik til Utdanningsetaten.

Også rutiner for rapportering av avvik, herunder for innmelding av avvik til Datatilsynet, var beskrevet på intranettet Tavla. Det framkom blant annet at Utdanningsetaten som behandlingsansvarlig skulle rapportere inn avvik så snart som mulig etter at avviket var oppdaget, og senest innen 72 timer.

6.2.2 Hauketo skole

Hauketo skole hadde ikke implementert rutinene for avviksbehandling som var tilgjengelig på Tavla. Skolens ledelse oppga at den ikke hadde gitt informasjon til de ansatte om håndtering av eventuelle hendelser og avvik. De oppga at dersom det oppsto en situasjon der noe gikk galt og personopplysninger kom på avveie, skulle informasjonen fjernes fra der den hadde vært tilgjengelig. Skolen hadde imidlertid ikke et system for å sikre at det ble gjort.

Skoleledelsen kom ikke på noen eksempler på at personopplysninger hadde kommet på avveie. Men de vurderte det som sannsynlig at dette likevel hadde skjedd, gitt risikoen for menneskelig svikt og antallet ansatte på skolen.

En av de ansatte vi snakket med, oppga at vedkommende ved en anledning hadde sendt en e-post som skulle til en elevs foresatte, til feil mottaker. Den ansatte oppga da å ha meldt ifra til rektor og til de berørte. Den aktuelle e-posten inneholdt ifølge den ansatte ikke noen sensitive opplysninger. Flere ansatte pekte på at det var takhøyde på skolen for å kunne ta opp slike forhold dersom det skjedde.

Da Kommunerevisjonen ble vist skolens systemer, ble det klart at tidligere adresse til en elev med hemmelig adresse lå tilgjengelig i det skoleadministrative systemet IST Everyday, herunder på den aktuelle elevens klasseliste. Elevens nye adresse framgikk ikke. Både tidligere og ny adresse var hemmelig. I etterkant av Kommunerevisjonens besøk, fikk vi bekreftet at skolen nå hadde fjernet adressen. Rektor oppga at skolen ikke hadde vurdert å melde avviket til Datatilsynet eller å varsle Utdanningsetaten sentralt.

Da Kommunerevisjonen gjennomførte undersøkelsen, ble vi også informert om en hendelse som hadde oppstått knyttet til Skolemeldingsappen. Hendelsen ble meldt til skolen av en berørt foresatt. Hendelsen innebar at en melding som gjaldt et bestemt barn, også automatisk ble sendt til barnets steforelder, selv om vedkommende ikke ble ført opp i kopifeltet. Skolen opplyste at den meldte fra til den eksterne driftsleverandøren om hendelsen, og at kopifeltet i skolemeldingsappen ble skrudd av for hele Osloskolen cirka to uker senere. En drøy uke etter dette ble en ny versjon av appen, der feilen var rettet, lansert. Skolen hadde ikke varslet saken til Utdanningsetaten sentralt eller til Datatilsynet. Skolen fant det fornuftig å varsle leverandøren, ettersom saken gjaldt en sentral applikasjon som skolen ikke hadde et eierskap til. Skolen oppga at den hadde fått informasjon fra Utdanningsetaten sentralt om at feil i slike applikasjoner skulle kommuniseres til driftsleverandørens «single point of contact» (eneste kontaktpunkt), og skolen forutsatte at driftsleverandøren meldte feilen videre til etaten. Utdanningsetaten sentralt oppga at etaten ble varslet om hendelsen i et forvaltningsmøte med leverandøren, og at funksjonaliteten da umiddelbart ble skrudd av. Ifølge etaten ble det som et langsiktig tiltak innført automatiske tester for denne funksjonen i Skolemeldingsappen. Etaten oppga at hendelsen ikke opprinnelig ble meldt til Datatilsynet, da sannsynligheten for at feilen skulle ha rammet mange foresatte, ble ansett å være liten. Etaten hadde imidlertid gjort en ny vurdering og planla å sende en avviksmelding til Datatilsynet i uke 45.

Etaten opplyste at den prøvde å få etablert en praksis der rektor selv vurderer og ev. melder personvernbrudd til Datatilsynet når avviket skyldes forhold som skolen er ansvarlig for, for eksempel feil gjort av ansatte. Avvik som skyldes feil i etatens systemer eller rutiner, for eksempel feil i virksomhetssystemer, skal varsles til Utdanningsetaten sentralt, som skal vurdere og ev. varsle Datatilsynet.

Etaten oppga videre at «single point of contact» hos den eksterne driftsleverandøren gjaldt skolenes IKT-ansvarliges kontakt ved tekniske problemer. I tilfeller der det var informasjonssikkerhet- og personvernhendelser det var snakk om, skulle skoleledelsen varsles, som igjen skulle varsle Utdanningsetaten sentralt, jf. sikkerhetsinstruksen for ansatte i skolen.

Kommunerevisjonen var i kontakt med leder for Foreldrerådets arbeidsutvalg (FAU) ved Hauketo skole, som ikke hadde noen innspill eller informasjon knyttet til skolens ivaretakelse av elevers personvern.

6.2.3 Nordseter skole

Ifølge skoleledelsen på Nordseter skole, hadde det vært hendelser og avvik knyttet til personvern. En typisk hendelse/avvik var e-postkorrespondanse med informasjon som ikke skulle vært sendt per e-post, for eksempel helseopplysninger, diagnoser e.l. Ifølge ledelsen startet slik korrespondanse gjerne med at en forelder tok kontakt med lærer per e-post og skrev sensitive personopplysninger i e-posten. I noen tilfeller fortsatte

korrespondansen uten at de sensitive opplysningene ble slettet. I noen tilfeller ble ledelsen etter hvert koblet på e-postkorrespondansen, slik at den oppdaget at e-postene inneholdt informasjon som ikke burde stått der. Det hadde ifølge ledelsen også hendt at foresatte hadde meldt ifra til skolen om at e-poster inneholdt informasjon som ikke skal sendes per e-post.

Etter slike hendelser/avvik var skolens rutine ifølge ledelsen å gjennomgå og evaluere hendelsen/avviket sammen med dem det gjaldt, herunder å vurdere om det var behov for oppfølging – for eksempel om tematikken skulle tas opp mer generelt med de ansatte på skolen.

Lærerne hadde ikke fått informasjon om hva de skulle gjøre dersom det oppsto en hendelse eller et avvik knyttet til elevers personopplysninger, utover at de måtte gi beskjed til ledelsen. Skoleledelsen opplevde at lærerne følte at de kunne komme til ledelsen hvis det oppsto feil, men mente at det nok var litt tilfeldig om dette ble gjort. Ifølge rektor hadde dette skjedd kun et par ganger i de årene han hadde vært rektor.

Skoleledelsen oppga at skolen ikke ville ha sendt avvik til Datatilsynet dersom en e-post med elevens initialer og lite sensitiv informasjon kom på avveie – dette ville ikke skolen vurdert det som et alvorlig avvik. Dersom det var snakk om en e-post med navn og «tunge» sensitive opplysninger, oppga rektor at han nok ville ha kontaktet Utdanningsetaten og forhørt seg med dem om hva skolen skulle gjøre videre. Skolen hadde ikke sendt varsel til Datatilsynet de årene rektor hadde vært rektor ved skolen. Når det gjaldt om skolen ville ha varslet den berørte om et avvik, oppga rektor at skolen ville ha forhørt seg med Utdanningsetaten om dette også.

Skolen hadde ikke en oversikt over hendelser og avvik knyttet til elevers personopplysninger. Det forelå heller ikke dokumentasjon på skolens håndtering av hendelser/avvik fra skoleårene 2020/2021 og 2021/2022. Skolen mente at den ikke hadde varslet Utdanningsetaten sentralt om slike avvik i denne perioden. Skoleledelsen visste ikke hvor hyppig hendelser og avvik knyttet til elevers personvern forekom, men fordi det var mange ansatte som håndterte personopplysninger om elever, vurderte de at dette var en kilde til mange mulige avvik. Etter skoleledelsens oppfatning var skolens system for å bruke hendelser og avvik i forbedringsarbeidet ikke godt nok.

Ingen av de ansatte vi snakket med, oppga at de kjente til at det hadde vært avvik eller hendelser knyttet til elevers personopplysninger de senere årene. Samtidig ble det pekt på forhold som ikke var bra, for eksempel at det hendte at teammøter og omtale av elever foregikk i rom som ikke var private, eksempelvis der det også var andre ansatte. De var ikke kjent med om skolen hadde et system for varsling og håndtering av slike avvik. Ansatte opplevde at det var takhøyde på skolen for å ta opp ting som går galt.

Da Kommunerevisjonen gjennomførte undersøkelsen, ble vi kjent med en praksis som innebar systematisk bruk av dårlige elev-passord i Feide for en del av elevene. Forholdet skyldtes praksis ved en annen (barne)skole enn Nordseter. Elevene tok med seg disse passordene da de startet på Nordseter skole. Siden elevene ikke hadde tofaktorautentisering i Feide, gjorde praksisen det enkelt å få tilgang til mange elevers innloggingsinformasjon – og dermed til en rekke opplysninger om disse elevene, herunder om fravær, karakterer, anmerkninger mv. Kommunerevisjonen tok samme dag som vi ble kjent med forholdet, dette opp med ledelsen på skolen, slik at de kunne følge

det opp. Skolen opplyste at den hadde informert alle elever og foresatte på ungdomstrinnet samt oppfordret dem til å gjøre endringer i passord. Videre oppga skolen at den hadde sendt en e-post til aktuelle lærere, som fikk ansvar for å ta opp saken i en time for å snakke litt om personvern og sikkerhet og i forlengelsen av det sterkt oppfordre elevene til å bytte passord. Forholdet ble fulgt opp av skolen cirka tre uker etter at Kommunerevisjonen gjorde skolen oppmerksom på det.

Kommunerevisjonen varslet også Utdanningsetaten sentralt om forholdet, slik at den kunne følge opp sårbarheten overfor andre skoler. På spørsmål om etaten hadde fulgt opp denne informasjonen, oppga etaten at den hadde fulgt opp informasjonen overfor den aktuelle barneskolen og fått bekreftelse fra skolen om at den nå hadde endret praksis for elevers passord. Videre oppga etaten at den hadde satt i gang en prosess for å sikre at ikke andre skoler hadde en dårlig praksis når det gjaldt elevers passord.

Kommunerevisjonen var i kontakt med leder for Foreldrerådets arbeidsutvalg (FAU) ved Nordseter skole, som ikke hadde noen innspill eller informasjon knyttet til skolens ivaretakelse av elevers personvern.

6.3 Kommunerevisjonens vurderinger

Skolene hadde tilgang til skriftlige rutiner fra Utdanningsetaten sentralt, som omhandlet håndtering av personvernavvik.

Verken Hauketo skole eller Nordseter skole hadde etablert tilfredsstillende rutiner og praksis på området.

Hauketo skole hadde ikke gitt informasjon om avvikshåndtering til lærerne. Kommunerevisjonen merker seg at skolen hadde fanget opp svært få personvernavvik, og stiller spørsmål ved om dette reflekterer det reelle antallet avvik. Skolen hadde heller ikke varslet Utdanningsetaten sentralt om de to avvikene som gjaldt Skolemeldingsappen og en elevs hemmelige adresse i IST Everyday.

Nordseter skole syntes å ha etablert en praksis for å følge opp hendelser der e-poster hadde inneholdt sensitive opplysninger, gjennom å ta opp hendelsen med involverte. Skolen hadde imidlertid ikke oversikt over hendelser/avvik ved skolen, heller ikke dokumentasjon på avvikene eller oppfølgingen av disse.

Kommunerevisjonen ser alvorlig på at det gikk nesten tre uker fra Nordseter skole fikk opplysninger om systematisk svake Feide-passord for en del elever før skolen iverksatte tiltak. Dette til tross for at personer med kjennskap til svakheten enkelt kunne få tilgang til mange elevers innloggingsinformasjon – og dermed til en rekke personopplysninger om disse elevene, herunder om sensitive forhold som fravær, karakterer, anmerkninger mv.

Mangelfulle rutiner og praksis ga risiko for at personvernavvik på de to skolene ikke ble fanget opp, forsvarlig lukket og fulgt opp. Mangelfull oppfølging gir risiko for at hendelser og avvik ikke blir benyttet i skolenes forbedringsarbeid, at de registrerte ikke varsles når det er nødvendig, og at ikke alle avvik blir meldt til Utdanningsetaten sentralt, slik at etaten kan vurdere aktuelle tiltak, herunder melding til Datatilsynet.

7. Kommunerevisjonens konklusjoner og anbefalinger

7.1 Konklusjoner

Kommunerevisjonen har undersøkt om personopplysninger om elever er tilstrekkelig sikret i skoler. Undersøkelsen har vært rettet mot Hauketo skole og Nordseter skole. I tillegg omfatter undersøkelsen en del om Utdanningsetaten sentralt sitt arbeid på flere områder, da det er en viktig del av rammene for skolenes arbeid, og oppgaver som ellers hadde ligget til den enkelte skole.

Undersøkelsen viser at det var iverksatt tiltak i Utdanningsetaten sentralt og på de to skolene for å bidra til en tilfredsstillende behandling av elevers personopplysninger. Utdanningsetaten hadde blant annet utarbeidet dokumentasjon med oversikt over behandling av elevers personopplysninger i systemer, apper mv. og gjennomført enkelte personvernkonsekvensvurderinger og flere risikoanalyser. De to skolene hadde også etablert rutiner som var egnet til å sikre at skoleledelsen hadde oversikt over de ansattes tilganger til informasjon i systemer i Skoleplattform Oslo, som IST Everyday, Itslearning, Teams, OneNote, Skolemelding mv. Dette ga også mulighet til å sikre at tilgangene var i samsvar med tjenstlig behov.

Samlet sett er det likevel Kommunerevisjonens konklusjon at personopplysninger om elever ikke ble behandlet tilfredsstillende ved Hauketo skole og Nordseter skole.

Denne konklusjonen bygger i hovedsak på følgende: De to skolene hadde ikke gjort vurderinger av om oversiktene over behandling av elevers personopplysninger som var utarbeidet av Utdanningsetaten sentralt, var dekkende for skolenes bruk av ulike systemer og tjenester. Utdanningsetaten hadde ikke ferdigstilt personvernkonsekvensvurderinger for læringsteknologien som var i bruk i Osloskolen, men arbeidet med dette. Skolene hadde heller ikke dokumenterte vurderinger av om det var risikoer forbundet med måten skolene benyttet systemene, herunder av hvordan skolen gjennomførte virksomhetsprosesser som involverte behandling av elevers personopplysninger. For eksempel hadde begge skolene prosesser for utarbeiding av individuelle opplæringsplaner og årsrapporter for elever med slike planer som omfattet særlige kategorier personopplysninger. Skolene hadde ikke gjennomført personvernkonsekvensvurderinger for disse prosessene. Lærerne ved skolene hadde ikke tilgang til Websak, og disse dokumentene ble behandlet i systemer som ikke var godkjent for slike personopplysninger. Dette kan også ha bidratt til en praksis ved begge skolene der lærere som ikke hadde tjenstlig behov, hadde tilgang til slike dokumenter. Det var også risiko for at skolene behandlet sensitive elevopplysninger i e-post, noe som forekom ved begge skolene.

Kommunerevisjonen mener det er uheldig at skolene manglet et verktøy for samhandling mellom ledelse og lærere for behandling av særlige kategorier personopplysninger. Kommunerevisjonen merker seg samtidig at Utdanningsetaten har oppgitt at den hadde igangsatt et langsiktig arbeid med anskaffelse av et slikt verktøy.

Videre hadde ikke Hauketo skole sikret tilfredsstillende opplæring i personvern for de ansatte ved skolen. Kommunerevisjonen stiller også spørsmål ved om opplæringen ved Nordseter skole var tilstrekkelig til å sikre alle ansatte tilfredsstillende kompetanse.

Verken Hauketo skole eller Nordseter skole hadde etablert tilfredsstillende rutiner og praksis for håndtering av personvernavvik. Det ga risiko for at personvernavvik ikke ble fanget opp, forsvarlig lukket og fulgt opp. Kommunerevisjonen ser alvorlig på at det gikk nesten tre uker fra Nordseter skole fikk opplysninger om systematisk svake Feide-passord for en del elever før skolen iverksatte tiltak. Dette til tross for at personer med kjennskap til svakheten enkelt kunne få tilgang til mange elevers innloggingsinformasjon – og dermed til en rekke personopplysninger om disse elevene, herunder om sensitive forhold som fravær, karakterer, anmerkninger mv.

Behandling av elevers personopplysninger som ikke er tilfredsstillende, innebærer at personvernrettighetene deres ikke i tilstrekkelig grad ivaretas. Dette gir risiko blant annet for at elevers personopplysninger slettes eller endres uautorisert eller kommer på avveie.

7.2 Anbefalinger

Kommunerevisjonen anbefaler at begge skolene iverksetter tiltak for å

- sikre at den har oversikt over sin behandling av personopplysninger, og at den gjennomfører nødvendige risikovurderinger og personvernkonsekvensvurderinger, når dette ikke er gjort av Utdanningsetaten sentralt
- sikre at tilgang til elevers personopplysninger er i tråd med tjenstlig behov
- sikre at ansatte har tilfredsstillende kompetanse når det gjelder ivaretakelse av elevers personvern
- sikre at personvernavvik blir tilfredsstillende håndtert, herunder fanget opp, lukket og fulgt opp

Utdanningsetaten sentralt utfører oppgaver knyttet til personvern og informasjons-sikkerhet som ellers ville ha ligget til den enkelte skole. Etatens arbeid er en viktig del av rammene for skolenes arbeid på området. Kommunerevisjonen anbefaler at Utdanningsetaten

- legger til rette for at skolene kan behandle særlige kategorier personopplysninger og andre sensitive personopplysninger på en tilfredsstillende måte, herunder i samhandlingen mellom lærere og ledelse
- viderefører arbeidet med å sikre at elevers personopplysninger ivaretas i Osloskolen
- følger opp de undersøkte skolenes forbedringsarbeid knyttet til deres behandling av elevers personopplysninger

Kommunerevisjonen anbefaler at byråden for oppvekst og kunnskap følger opp Utdanningsetatens forbedringsarbeid knyttet til etatens behandling av elevers personopplysninger.

8. Uttalelser til rapporten og Kommunerevisjonens vurderinger av disse

Kommunerevisjonen har bedt om og mottatt uttalelser fra Byrådsavdeling for oppvekst og kunnskap, Utdanningsetaten, Hauketo skole og Nordseter skole. Utdanningsetaten og de to skolene avga en felles uttalelse. I dette kapittelet presenteres og vurderes vesentlige momenter i uttalelsene. Uttalelsene følger i sin helhet i vedleggene 3 og 4.

8.1 Byrådsavdeling for oppvekst og kunnskap

8.1.1 Byrådsavdelingens uttalelse

Byrådsavdelingen skriver at rapporten oppleves som nyttig, og at den peker på viktige forbedringspunkter i det videre arbeidet på området. Byrådsavdelingen har ingen kommentarer til revisjonskriterier eller metoden med tanke på rapportens konklusjoner. Byrådsavdelingen peker på at Kommunerevisjonen har undersøkt praksis ved to utvalgte skoler og noe av Utdanningsetatens sentrale arbeid. Byrådsavdelingen skriver at det naturlig nok er vanskelig å si noe om hvor representative funnene er for de andre skolene i Oslo, men at det uansett ligger viktige læringspunkter i rapporten.

Byrådsavdelingen peker på at Utdanningsetaten har prioritert arbeid med informasjonssikkerhet og personvern høyt de siste årene og at byrådsavdelingen ser at det gir resultater. Byrådsavdelingen mener det derfor er grunn til å tro at noe kan ha blitt forbedret siden undersøkelsesperioden. Videre skriver byrådsavdelingen at håndtering av personopplysninger er en stor utfordring for skolene, og at det etter byrådsavdelingens vurdering er hensiktsmessig at Utdanningsetaten i så stor grad som mulig legger til rette for at personvern blir godt håndtert ute i skolene.

Når det gjelder tiltak, skriver byrådsavdelingen at den allerede har en tett dialog med Utdanningsetaten for å følge opp arbeidet med personvern i skolesektoren. Byrådsavdelingen vil som en del av denne dialogen følge opp arbeidet med konklusjonene fra rapporten. Ifølge byrådsavdelingen er personvern tema i styringsdialogen gjennom etatsstyringsmøter samt gjennom rapportering av ledelsens gjennomgang og virksomhetsleders egenerklæring og eget møte i forbindelse med rapporteringen. Når det gjelder tidsperspektiv for tiltaket, skriver byrådsavdelingen at oppfølgingen av Utdanningsetatens forbedringsarbeid er et kontinuerlig og langsiktig arbeid.

8.1.2 Kommunerevisjonens vurdering

Byrådsavdelingen varsler tiltak som er relevant for rapportens anbefaling til byråden. Kommunerevisjonen har for øvrig ingen kommentarer til byrådsavdelingens uttalelse.

8.2 Utdanningsetaten, Hauketo skole og Nordseter skole

8.2.1 Etaten og skolenes uttalelse

Utdanningsetaten oppfatter at rapporten er nyttig for videre utviklingsarbeid, og en god kvalitetssikring av etatens pågående arbeid innen informasjonssikkerhet og personvern. Etaten og skolene har ingen kommentarer til prosjektets revisjonskriterier, metode, anvendte kilder eller data.

Utdanningsetaten skriver at den vi fortsette å jobbe for å bedre elevenes personvern i Osloskolen. Etaten vil gjennomgå Kommunerevisjonens anbefalinger grundig og lage en prioritert oppfølgingsplan. Hauketo skole og Nordseter skole planlegger følgende tiltak:

- Opplæring av nyansatte (fra og med høsten 2023)
- Opplæring av alle ansatte (iverksatt og videreføres)
- Skriftliggjøring av rutiner (januar–juni 2023)
- Rutiner for risikovurdering av innsamling og lagring av personverninformasjon (kontinuerlig)
- Rutiner for avvikshåndtering informeres om og iverksettes (januar–mars 2023)

Utdanningsetaten har som mål å starte opp de fleste tiltakene i løpet av 2023. Nordseter skole skriver at arbeidet begynner vår 2023, og skal være formalisert og gjort kjent for ansatte innen skolestart høsten 2023.

8.2.2 Kommunerevisjonens vurdering

Kommunerevisjonen merker seg at Utdanningsetaten og de to skolene samlet sett varsler tiltak, deriblant å gjennomgå anbefalingene grundig og lage en prioritert oppfølgingsplan. Kommunerevisjonen forstår dette som at etaten vil iverksette tiltak til alle anbefalingene. Kommunerevisjonen har ingen kommentarer for øvrig til uttalelsen.

Referanser

Referanser fra Oslo kommune

Byrådssak 1070/15 *Instruks for virksomhetsstyring i Oslo kommune*[7]

Byrådssak 1105/13 *Instruks for informasjonssikkerhet for Oslo kommune*

Byrådssak 1099/10 *Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet i Oslo kommune*

Tildelingsbrev til Utdanningsetaten for 2020 og 2021

Utdanningsetatens årsberetning for 2020

Eksterne referanser

Datatilsynet (2019) *Vurdering av personvernkonsekvenser (DPIA)* (veiledning), sist endret 17.07.2019

Datatilsynet (2019) *Hva er personvern?*, tilgjengelig på https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/, sist endret 17.07.2019

Lov 15. juni 2018 nr. 38: Lov om behandling av personopplysninger (personopplysningsloven)

For 23. juni 2006 nr. 724: Forskrift til opplæringslova (endring fra 1. august 2021)

[7] Ny *Instruks for virksomhetsstyring i Oslo kommune* trådte i kraft fra 7. april 2022, jf. sak 1036/22

Vedlegg 1 Revisjonskriterier

I det følgende gir vi en oversikt over revisjonskriteriene som Kommunerevisjonen har lagt til grunn i forvaltningsrevisjonen. Vi går også gjennom kildene for de ulike kriteriene.

Revisjonskriterier er de kravene og forventningene Kommunerevisjonen legger til grunn for sine vurderinger. Revisjonskriteriene er utledet fra autoritative kilder i tråd med *Standard for forvaltningsrevisjon* (RSK 001). I denne undersøkelsen er revisjonskriteriene i hovedsak utledet/hentet fra personopplysningsloven inkl. personvernforordningen, forskrift til opplæringsloven, Datatilsynets veileder om personvernkonsekvensvurderinger (DPIA), Oslo kommunes instruks for informasjonssikkerhet og kommunens instruks for virksomhetsstyring.

Problemstillingen i undersøkelsen har vært følgende:
- Er personopplysninger om elever tilstrekkelig sikret i skolene?

For å besvare problemstillingen har vi undersøkt følgende temaer:
- kartlegging av informasjonsverdier og risikovurdering og -håndtering
- tilgangsstyring
- opplæring og kompetanse
- avvikshåndtering

Forvaltningsrevisjonen har vært innrettet for å revidere praksis ved de to utvalgte skolene. Undersøkelsen omfatter i tillegg en del om Utdanningsetaten sentralt sitt arbeid på flere områder, da det er en viktig del av rammene for skolenes arbeid, og oppgaver som ellers hadde ligget til den enkelte skole.

Kartlegging av informasjonsverdier og risikovurdering og -håndtering:

Kommunerevisjonen har lagt følgende revisjonskriterier til grunn:
- Skolen skal ha oversikt over sin behandling av elevenes personopplysninger. Oversikten skal være dokumentert.
- Sannsynlige personvernkonsekvenser skal vurderes før behandling starter. Vurderingen skal være dokumentert. Dersom det er sannsynlig at behandlingen kan medføre høy risiko, skal dette gjøres i form av en personvernkonsekvensvurdering (DPIA – Data Protection Impact Assessment).
- Risikoen for informasjonssikkerhetshendelser knyttet til behandling av personopplysninger om elever skal vurderes. Risikovurderingen skal være dokumentert.

Vi har lagt til grunn at de ovennevnte prosessene kan ivaretas av enten Utdanningsetaten sentralt eller av de enkelte skolene.

Kriteriene er utledet fra følgende kilder:
Personvernforordningen er gjennomført i norsk lov gjennom personopplysningsloven som trådte i kraft 20. juli 2018. I forordningens artikkel 30 stilles det krav om at det føres protokoll over behandlingsaktiviteter:

Artikkel 30.Protokoller over behandlingsaktiviteter

1. Hver behandlingsansvarlig og, dersom det er relevant, den behandlingsansvarliges representant skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Nevnte protokoll skal inneholde følgende informasjon:

a) navnet på og kontaktopplysningene til den behandlingsansvarlige og, dersom det er relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet,

b) formålene med behandlingen,

c) en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger,

d) kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner,

e) dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1 annet ledd, dokumentasjon på nødvendige garantier,

f) dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger,

g) dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1.

2. Hver databehandler og, dersom det er relevant, databehandlerens representant skal føre en protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av en behandlingsansvarlig, og som skal inneholde:

a) navnet på og kontaktopplysningene til databehandleren eller databehandlerne og til hver behandlingsansvarlig som databehandleren opptrer på vegne av, samt, dersom det er relevant, den behandlingsansvarliges eller databehandlerens representant og personvernombudet,

b) kategoriene av behandling utført på vegne av hver behandlingsansvarlig,

c) dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1 annet ledd, dokumentasjon på nødvendige garantier,

d) dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1.

3. Protokollene nevnt i nr. 1 og 2 skal være skriftlige, herunder elektroniske. (...)

I personvernforordningen artikkel 24, 25, 32 og 35 framkommer det krav om at det gjennomføres risikovurdering og vurdering av sannsynlige personvernkonsekvenser:

Artikkel 24. Den behandlingsansvarliges ansvar

1. Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

Artikkel 25. Innebygd personvern og personvern som standardinnstilling

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.

Artikkel 32. Sikkerhet ved behandlingen

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet, (...)

2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Artikkel 35.Vurdering av personvernkonsekvenser

1. Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.
(...)

7. Vurderingen skal minst inneholde

a) en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige,

b) en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene,

c) en vurdering av risikoene for de registrertes rettigheter og friheter som nevnt i nr. 1, og

d) de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at denne forordning overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser.

(...)

> 11. Ved behov skal den behandlingsansvarlige foreta en gjennomgåelse for å vurdere om behandlingen utføres i samsvar med vurderingen av personvernkonsekvenser, i det minste dersom risikoen som behandlingen medfører, endres.

Krav om risikovurdering framkommer også i Oslo kommunes instruks for informasjonssikkerhet og instruks for virksomhetsstyring, jf. nedenfor:

Byrådssak 1105/13 *Instruks for informasjonssikkerhet i Oslo kommune*
Punkt 3.3

> Risikovurdering skal være en sentral del av arbeidet med sikkerhetstiltak. Konkrete sikkerhetstiltak skal bygge på anbefalte sikkerhetskrav i mal for egenerklæring og dokumenterte risikovurderinger.

Punkt 4.2

> Alle virksomheter må kartlegge og verdivurdere informasjon som må beskyttes i henhold til integritet, konfidensialitet eller tilgjengelighet.

Punkt 4.3

> Oversiktene over rettslige krav og verdivurdert informasjon må brukes som grunnlag for vurdering og prioritering av sikkerhetstiltak i den enkelte virksomhet og for fellesystemer, sektorsystemer og andre ikke-virksomhetsspesifikke systemer.

Byrådssak 1070/15 *Instruks for virksomhetsstyring i Oslo kommune*
Punkt 5.7.2

> Risikovurderinger skal utgjøre en sentral del av grunnlaget for å velge ut relevante sikkerhetstiltak. Vurdering av trusler og sårbarhet må inngå i dette arbeidet. Virksomhetens tiltak for å ivareta informasjonssikkerhet skal dokumenteres.

Datatilsynets veiledning om DPIA: *Vurdering av personvernkonsekvenser (DPIA)* (sist endret 17.07.2019):

> **Datatilsynets liste over behandlingsaktiviteter som alltid krever at det gjennomføres en DPIA**
>
> (...)
>
> - Behandling av personopplysninger for å evaluere læring, mestring og trivsel i skoler eller barnehager. Dette inkluderer alle utdanningsnivåer, fra barne- og ungdomsskole, videregående skoler og høyere utdanning. (Sårbare registrerte og systematisk monitorering.)
> - (...)
> - Kameraovervåking i skoler og barnehager i åpningstider. (Systematisk monitorering og sårbare registrerte)

Tilgangsstyring

Kommunerevisjonen har lagt følgende revisjonskriterier til grunn:

- Skolen skal ha oversikt over hvem som har tilgang til personopplysninger om elever, både materielt og i IT-systemer.
- Tilgang til personopplysninger om elever skal være i samsvar med tjenstlig behov.

Kommunerevisjonen har lagt til grunn at det skal være etablert rutiner og praksis for en tilfredsstillende tilgangsstyring i de utvalgte systemene. Rutiner for tilfredsstillende tilgangsstyring bør omfatte blant annet tildeling, endring og gjennomgang av tilganger.

Kriteriene er utledet fra følgende kilder:
Personvernforordningen
artikkel 5 punkt 1f:

> Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»).

Forskrift til opplæringslova § 22A-2 Krav til tilgangsstyring (fra 1. august 2021)

> Kommunar og fylkeskommunar skal sørgje for tilgangsstyring slik at dei som arbeider for verksemda, berre har tilgang til personopplysningar dersom og i den utstrekning dei treng opplysningane for formål som nemnde i opplæringslova § 15-10. Kommunar og fylkeskommunar skal sørgje for at den som arbeider for verksemda, har nødvendig kunnskap om personvern og informasjonstryggleik før vedkommande får tilgang til personopplysningar.
>
> Krava i første ledd gjeld personopplysningar som er omfatta av personopplysningsloven, og som blir behandla med heimel i opplæringslova

Instruks for virksomhetsstyring i Oslo kommune (byrådssak 1070/15) punkt 5.7.1:

> Informasjonssikkerhetsarbeidet i kommunen skal baseres på klar fordeling av roller og ansvar internt i virksomheten og overfor databehandlere, intern leverandør og eventuelle andre instanser som ivaretar informasjonssikkerhetsoppgaver for virksomheten.

Instruks for informasjonssikkerhet for Oslo kommune (byrådssak 1105/13) punkt 5.2 og 5.3:

> 5.2 Fysisk sikring
>
> a) Alle virksomheter må iverksette nødvendige tiltak for å hindre uvedkommende adgang til virksomhetens informasjonsverdier.
>
> b) Alle virksomheter må iverksette tiltak for å avverge og redusere skade på informasjon og IKT-utstyr som følge av uautorisert adgang eller miljømessige trusler som f. eks. brann eller vannskader.
>
> 5.3 Tilgangskontroll
>
> a) All tilgang til informasjon og systemer i Oslo kommune skal være i samsvar med tjenstlig behov. Det innebærer vurdering og bruk av tiltak som f. eks.
>
> 1. Autentiseringsmekanismer i systemene
>
> 2. Autoriseringsprosesser ved tildeling, endring og avslutning av tilgang
>
> 3. Sikring av bærbart utstyr
>
> 4. Sikring av tilgangskontroll i nettverk. Dette gjelder blant annet begrensning og kontroll av systemverktøy for overstyring, identifikasjon av utstyr, dedikerte soner for sensitive personopplysninger og annen informasjon som krever særskilt konfidensialitetsbeskyttelse.

Opplæring og kompetanse

Kommunerevisjonen har lagt følgende revisjonskriterium til grunn:

- Skolen skal sørge for at de ansatte ved skolen har tilfredsstillende kompetanse til å kunne ivareta elevenes personvern.

Kriteriet er utledet fra følgende kilder:

Forskrift til opplæringslova § 22A-2 Krav til tilgangsstyring (fra 1. august 2021)

> Kommunar og fylkeskommunar skal sørgje for tilgangsstyring slik at dei som arbeider for verksemda, berre har tilgang til personopplysningar dersom og i den utstrekning dei treng opplysningane for formål som nemnde i opplæringslova § 15-10. Kommunar og fylkeskommunar skal sørgje for at den som arbeider for verksemda, har nødvendig kunnskap om personvern og informasjonstryggleik før vedkommande får tilgang til personopplysningar.
>
> Krava i første ledd gjeld personopplysningar som er omfatta av personopplysningsloven, og som blir behandla med heimel i opplæringslova

Byrådssak 1099/10 *Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet i Oslo kommune*
§ 8 Informasjonssikkerhet (ansvar og oppgaver):

> (1) *Ansvar*:
>
> Den enkelte leder har ansvar for informasjonssikkerheten i egen virksomhet.
>
> (2) *Oppgaver*:
>
> Innen virksomhetsleders ansvar for informasjonssikkerhet ligger bl.a. følgende oppgaver:
>
> 1) ivareta informasjonssikkerhet og intern kontroll i henhold til personopplysningsloven, annen lovgivning og kommunens eget regelverk
>
> (...)
>
> 4) sørge for at krav til informasjonssikkerhetskompetanse defineres og følges opp i egen virksomhet

Byrådssak 1070/15 *Instruks for virksomhetsstyring i Oslo kommune*
Punkt 5.3 og punkt 5.3.3

> **5.3 Virksomhetsstyringen skal sikre at kommunen overholder lover og regelverk, foretar korrekt saksbehandling og ivaretar kommunens rettslige posisjon**
>
> (...)
>
> 5.3.3 Alle virksomheter skal ha eller innhente tilstrekkelig kompetanse til å ivareta korrekt saksbehandling og til å ivareta kommunens rettslige posisjon, herunder også privatrettslig posisjon.

Punkt 5.8 og 5.8.8

> **5.8 God personalpolitikk, godt arbeidsmiljø, effektive arbeidsprosesser og god ressursanvendelse skal være integrert i virksomhetsstyringen**
>
> (...)
>
> 5.8.8 Virksomheten skal til en hver tid sørge for å ha tilstrekkelig kompetanse for å ivareta sine oppgaver. Kompetanseutvikling skal rettes mot strategisk viktige kompetanseområder.

Byrådssak 1105/13 *Instruks for informasjonssikkerhet for Oslo kommune*
Punkt 3.4

3.4 Det er en del av lederansvaret å sørge for at ansatte kjenner sitt ansvar for informasjonssikkerhet i henhold til de oppgavene de har.

Tildelingsbrev til Utdanningsetaten 2021:

Informasjonssikkerhet og personvern

Skolene behandler store mengder personopplysninger om mange elever, foresatte og ansatte. Regelverket på dette området stiller høye krav til kunnskap og kompetanse om personvern i hele skolesektoren, fra leverandører og helt ned på brukernivå og det er viktig at UDE jobber systematisk for å øke kompetansen og sørge for at det gjøres gode vurderinger knyttet til alle digitale løsninger som behandler personopplysninger. (...)

Avvikshåndtering

Kommunerevisjonen har lagt følgende revisjonskriterier til grunn:

- Skolen skal ha rutiner og praksis for å håndtere hendelser og avvik knyttet til informasjonssikkerhetshendelser som rammer personopplysninger om elever.
- Skolens håndtering av hendelser og avvik knyttet til elevers personopplysninger skal være dokumentert.

Kriteriet er utledet fra følgende kilder:

Personvernforordningen artikkel 33 og 34 omhandler håndtering av avvik knyttet til informasjonssikkerhet:

Artikkel 33. Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten

1. Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet i samsvar med artikkel 55, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis.

2. Etter å ha fått kjennskap til et brudd på personopplysningssikkerheten skal databehandleren uten ugrunnet opphold underrette den behandlingsansvarlige.

3. Meldingen nevnt i nr. 1 skal minst

a) beskrive arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,

b) inneholde navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes,

c) beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,

d) beskrive de tiltak som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

4. Dersom og i den grad det ikke er mulig å gi all informasjon samtidig, kan den gis trinnvis uten ytterligere ugrunnet opphold.

5. Den behandlingsansvarlige skal dokumentere ethvert brudd på personopplysningssikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det. Denne dokumentasjonen skal gjøre det mulig for tilsynsmyndigheten å kontrollere samsvar med denne artikkel

Artikkel 34.Underretning av den registrerte om brudd på personopplysningssikkerheten

1. Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet.

2. Underretningen til den registrerte nevnt i nr. 1 i denne artikkel skal inneholde en klar og tydelig beskrivelse av arten av bruddet på personopplysningssikkerheten og minst informasjonen og tiltakene nevnt i artikkel 33 nr. 3 bokstav b), c) og d).

3. Underretningen til den registrerte nevnt i nr. 1 er ikke påkrevd dersom noen av følgende vilkår er oppfylt:

a) den behandlingsansvarlige har gjennomført egnede tekniske og organisatoriske sikkerhetstiltak, og disse tiltakene er blitt anvendt på personopplysningene som er berørt av bruddet på personopplysningssikkerheten, særlig tiltak som gjør personopplysningene uleselige for enhver person som ikke har autorisert tilgang til dem, f.eks. kryptering,

b) den behandlingsansvarlige har truffet etterfølgende tiltak som sikrer at det ikke lenger er sannsynlig at den høye risikoen for de registrertes rettigheter og friheter nevnt i nr. 1 vil oppstå,

c) det vil innebære en uforholdsmessig stor innsats. Dersom dette er tilfellet, skal allmennheten isteden underrettes, eller det skal treffes et lignende tiltak som sikrer at de registrerte underrettes på en like effektiv måte.

4. Dersom den behandlingsansvarlige ikke allerede har underrettet den registrerte om bruddet på personopplysningssikkerheten, kan tilsynsmyndigheten, etter å ha vurdert sannsynligheten for at bruddet vil medføre en høy risiko, kreve at den behandlingsansvarlige gjør dette, eller beslutte at ett eller flere av vilkårene nevnt i nr. 3 er oppfylt

Instruks for informasjonssikkerhet for Oslo kommune (byrådssak 1105/13)

Punkt 5.6:

Hendelseshåndtering

a) Varsling og håndtering av hendelser (avvik, feilsituasjoner eller fare for slike) skal skje så nær hendelsen som mulig, og i henhold til dokumenterte rutiner for varsling og håndtering.

b) Det skal være enhetlige rutiner for etterfølgende rapportering av hendelser.

c) Rutiner for varsling og håndtering av hendelser knyttet til forvaltning eller drift av systemer må foreligge fra systemeier for så vidt gjelder fellessystemer, sektorsystemer og tverrsektorielle systemer.

Tildelingsbrev til Utdanningsetaten 2020:

Informasjonssikkerhet – personvern

Virksomhetenes arbeid med å etterleve krav til informasjonssikkerhet og personvern må fortsette. (...) Tilstrekkelig styring og kontroll av informasjonssikkerheten, herunder rutiner for (...) hendelses- og avvikshåndtering, er vesentlig.

Vedlegg 2 Metode

1.1 Generelt om forvaltningsrevisjon

De sentrale delene av en forvaltningsrevisjon er beskrevet i *Standard for forvaltningsrevisjon* fra NKRF (RSK 001 *Standard for forvaltningsrevisjon*). Disse delene er like for alle forvaltningsrevisjoner. Kort oppsummert bestemmer kontrollutvalget problemstillingen i sin bestilling til Kommunerevisjonen. Kommunerevisjonen utleder relevante revisjonskriterier for problemstillingen. Kriteriene er målestokken som vi holder den reviderte enheten opp mot. For å svare på spørsmålet om enheten når de gitte målene/revisjonskriteriene, samler vi inn relevante data som vi bearbeider og analyserer. Dette gir oss et faktagrunnlag som vi vurderer opp mot revisjonskriteriene. Vurderingene leder fram til Kommunerevisjonens konklusjoner og eventuelle anbefalinger.

1.2 Beskrivelse av prosjektgjennomføring

Undersøkelsen omfatter Hauketo skole og Nordseter skole. I tillegg er Utdanningsetatens arbeid på noen punkter omtalt/undersøkt.

Brev om oppstart av forvaltningsrevisjonen ble sendt til Utdanningsetaten og byråden for oppvekst og kunnskap 16. desember 2021. På grunn av koronapandemien og dens konsekvenser for skolene rundt nyttår ble undersøkelsen satt på vent en periode. I april 2022 ble det besluttet å starte opp igjen undersøkelsen, og oppstartsbrev ble sendt til Hauketo skole og Nordseter skole 22. april 2022. Oppstartsmøter ble avholdt med Utdanningsetaten og Byrådsavdeling for oppvekst og kunnskap 4. april 2022 (videomøte), med Nordseter skole 5. mai 2022 og med Hauketo skole 6. mai 2022.

Kommunerevisjonen sendte et utkast til revisjonskriterier til Utdanningsetaten og Byrådsavdeling for oppvekst 22. april 2022 og til Nordseter skole og Hauketo skole henholdsvis 5. mai 2022 og 6. mai 2022. Det kom ingen merknader til revisjonskriteriene.

Datainnsamlingen ble i hovedsak gjennomført i perioden mai–september 2022. Vi sendte faktabeskrivelse til verifisering hos virksomhetene 31. oktober 2022. Vi ga en presentasjon av Kommunerevisjonens vurderinger og konklusjoner i møte 2. desember 2022.

Rapporten ble sendt til uttalelse til byråden for oppvekst og kunnskap, Utdanningsetaten, Hauketo skole og Nordseter skole 9. desember. Kommunerevisjonen mottok svar fra Utdanningsetaten, Hauketo skole og Nordseter skole i brev 5. januar 2023 og fra byrådsavdelingen i brev 13. januar 2023. Det er gjort korrigeringer i rapporten som følge av korrektur.

1.3 Metode for datainnhenting

Som nevnt over er undersøkelsen gjennomført på to utvalgte skoler: Hauketo skole og Nordseter skole. Skolene ble ikke valgt med utgangspunkt i forhåndskunnskap om risiko, men valgt skjønnsmessig ut fra at vi ønsket en 1.–10.-skole og en 8.–10.-skole og to skoler med noe ulikt elevgrunnlag.

Undersøkelsen er i hovedsak basert på informasjon innhentet gjennom dokumentgjennomgang og intervjuer. I tillegg har vi blitt vist hvordan ulike prosesser som omfatter elevenes personopplysninger, gjennomføres i de to skolene. Vi stilte også skriftlige spørsmål til skolene og etaten i forbindelse med datainnsamlingen og ved verifisering av fakta.

Undersøkelsesperioden har i utgangspunktet vært skoleåret 2020–2021 og 2021–2022, men på en rekke punkter har det vært naturlig å beskrive og vurdere praksis på observasjonstidspunktet.

Under følger nærmere informasjon om metodene som er brukt i prosjektet:

1.3.1 Møter og intervjuer

For å få informasjon om Utdanningsetatens arbeid knyttet til ivaretakelse av elevers personvern, hadde vi møter med henholdsvis seniorkonsulent informasjonssikkerhet / informasjonssikkerhetskoordinator og lederen for personverngruppa i etaten. Vi skrev referater fra begge møtene, og referatene ble verifisert.

For å få informasjon om hvordan Hauketo skole og Nordseter skole arbeidet med å ivareta elevers personopplysninger, herunder i ulike virksomhetsprosesser, i opplæring av ansatte mv., gjennomførte vi flere intervjuer ved begge skolene. Følgende ansatte har blitt intervjuet:

- rektor og assisterende rektor
- ansatt ved kontoret
- rådgiver
- IKT-ansvarlig
- to lærere

Alle intervjuene var semistrukturerte. Det vil si at vi hadde utformet hovedspørsmålene på forhånd, og at vi stilte oppfølgende spørsmål underveis der det var behov. Informantene hadde også anledning til å fortelle om andre forhold de anså som relevante for undersøkelsen. Referatene fra intervjuene ble verifisert av hver enkelt informant.

I tillegg gjennomførte vi en samtale med to elevrådsrepresentanter ved begge skolene for å få informasjon fra dem om bruken av IKT-verktøy og lignende. I forkant av disse samtalene sendte vi skriftlig informasjon om undersøkelsen til både de aktuelle elevene og deres foresatte. Ved den ene skolen kontaktet vi de aktuelle direkte, og ved den andre skolen ble informasjonen sendt ut via skolen. Vi innhentet også skriftlig samtykke fra elevenes foresatte til at elevene kunne delta.

Vi var også i e-postkontakt med lederen for foreldrerådets arbeidsutvalg (FAU) ved begge skolene med spørsmål om de hadde innspill eller informasjon om skolens ivaretakelse av elevers personvern. Vi fikk tilbakemelding per e-post.

Ved Nordseter skole gikk rektor ut i permisjon, og en assisterende rektor sluttet ved skolen, henholdsvis fra august 2022 og medio november 2022.

1.3.2 Dokumentasjon

Vi har også gjennomgått relevant dokumentasjon fra Utdanningsetaten, Hauketo skole og Nordseter skole. Dokumentasjonen fra Utdanningsetaten omfattet blant annet rutinebeskrivelser og informasjonsmateriell på etatens internettsider og intranett, risikovurderinger, system- og prosessoversikter med verdivurderinger og med informasjon om behandling av personopplysninger og overordnede og systemspesifikke personvernvurderinger. Denne dokumentasjonen ble gjennomgått for å belyse områder som utgjør rammer for skolenes arbeid med ivaretakelse av elevenes personvern og av oppgaver som ellers ville ligget til de undersøkte skolene.

Dokumentene fra skolene omfattet blant annet overordnede strategidokumenter og ulike risikovurderinger. Denne ble gjennomgått for å identifisere forhold av betydning for skolenes praksis knyttet til ivaretakelse av elevenes personvern. Vi mottok og gjennomgikk også annen dokumentasjon, knyttet til blant annet opplæring og til skolenes føringer til ansatte om bruk av ulike læringsteknologiske apper og tjenester.

1.4 Behandling av personopplysninger

Formålet med Kommunerevisjonens innhenting, behandling og oppbevaring av personopplysninger er å utføre den lovbestemte revisjonen av Oslo kommune. Hvilke personopplysninger vi samler inn og behandler, avhenger av hvilken informasjon vi trenger for å gjennomføre undersøkelsen. Personopplysningene vil kunne være opplysninger som kommunen er pålagt å innhente, som av andre grunner er i kommunens systemer, som ansatte plikter å oppgi til Kommunerevisjonen, eller som er gitt frivillig.

Kommunerevisjonen følger bestemmelsene i personopplysningsloven og legger vekt på å begrense lagringen av personopplysninger. Vi legger vekt på bare å innhente data som er relevante for formålet med undersøkelsen. Vi tar bare vare på personopplysninger som er nødvendige for dokumentasjon av arbeidet vi utfører. Personopplysninger lagres utilgjengelig for uvedkommende.

Retten til å få slettet personopplysninger er bl.a. styrt av at Kommunerevisjonen har 10 års lagringsplikt for dokumentasjon av revisjonene.

For ytterligere informasjon om Kommunerevisjonens ansvar for og behandling av personopplysninger, se vår personvernerklæring.[8]

I denne undersøkelsen har vi ikke innhentet personopplysninger via dokumenter eller digitale formater, utover opplysninger som respondenter har gitt i intervjuer, og som er nedtegnet i verifiserte referater. Dette vil typisk dreie seg om respondentens personalia og deres synspunkter på ulike forhold som var tema for intervjuene. Disse referatene er håndtert i tråd med Kommunerevisjonens retningslinjer og praksis for behandling av personopplysninger. I tillegg har Kommunerevisjonene gjennom observasjoner av IKT-systemer i de utvalgte skolene blitt eksponert for elevers personopplysninger. Disse har ikke blitt nedtegnet eller på annen måte behandlet ut over den omtalte observasjonen.

[8] https://www.oslo.kommune.no/getfile.php/13292652-1535640780/Tjenester%20og%20tilbud/Politikk%20og%20administrasjon/Etater%2C%20foretak%20og%20ombud/Kommunerevisjonen/Personvernerkl%C3%A6ring%20for%20Kommunerevisjonen.pdf

1.5 IT-rettede kontroller

Undersøkelsen har i hovedsak vært rettet mot forhold knyttet til skolenes bruk av og kontroll med digitale verktøy, slik at de fleste kontrollhandlingene er IT-rettede. Undersøkelsen har ikke omfattet teknisk testing, utover at det i noen tilfeller er gjort observasjoner i skolenes IKT-miljø av funksjoner av betydning for skolenes behandling av elevenes personopplysninger. Dette ble primært gjort ved at vi ba respondenter vise oss elementer i IT-miljøet vi hadde fått informasjon om, slik at vi kunne forsikre oss om at vi hadde oppfattet informasjonen korrekt. Dette kunne for eksempel dreie seg om påloggingsprosedyrer eller på hvilken måte ulike personopplysninger var registrert og framgikk i et system.

1.6 Gyldighet og pålitelighet

For å kvalitetssikre datagrunnlaget har vi vurdert dataenes validitet (gyldighet) og reliabilitet (pålitelighet). Gyldighet refererer til hvor godt man klarer å måle det man har til hensikt å måle eller undersøke. Pålitelighet refererer til hvor nøyaktig innsamlingen av data har vært.

Forvaltningsrevisjonens hovedproblemstilling er undersøkt gjennom å vurdere skolenes praksis innen en rekke temaer. Temaene er valgt ut for å gi et godt bilde av vesentlige sider ved hovedproblemstillingen, men det vil også kunne finnes andre mulige forhold av betydning som kunne vært undersøkt. Kommunerevisjonens vurderinger og konklusjoner gjelder de undersøkte områdene og ikke eventuelle andre forhold. Undersøkelsen av temaene bygger på revisjonskriterier som på et tidlig stadium ble forelagt for Byrådsavdeling for oppvekst og kunnskap, Utdanningsetatens administrasjon og de undersøkte skolene. Ingen av disse hadde innsigelser til kriteriene. Kommunerevisjonen har valgt ut og gjennomført kontrollhandlinger for å få tilstrekkelig informasjon om skolenes praksis på de undersøkte områdene.

Denne undersøkelsen bygger på data fra ulike datakilder. Gjennom de ulike formene for datainnsamling har vi, så langt det har latt seg gjøre, hatt flere kilder til opplysninger om de samme forholdene. Disse opplysningene er så sammenholdt for å sikre at opplysningene gir et korrekt bilde av skolenes praksis. I den grad vi i faktabeskrivelsen gjengir opplysninger som det innenfor undersøkelsens rammer ikke har vært mulig eller hensiktsmessig å triangulere, informerer vi om typen kilde i den løpende teksten.

Mye av dokumentasjonen som er benyttet i undersøkelsen, er hentet fra Utdanningsetatens internettsider og intranett. I hovedsak oppgis publiseringsdato og dato for siste endring i dokumentene, men vi har ikke innhentet tidligere versjoner av disse dokumentene. Det er derfor risiko for at dokumenter er endret i løpet av undersøkelsesperioden. Dette vil ikke være unaturlig, da informasjonen bør være oppdatert. Alle revisjonsbevis er derfor ikke nødvendigvis valide for hele perioden, slik at våre vurderinger og konklusjoner i stor grad er basert på status på observasjonstidspunktet. For dokumenter som er innhentet direkte fra Utdanningsetaten og de undersøkte skolene, har vi i enkelte tilfeller sjekket samsvar mellom dokumentets metainformasjon og informasjon vi mottok om dokumentets historikk og status.

Intervjureferater er verifisert av dem som ble intervjuet. Hele faktabeskrivelsen er verifisert ved at Utdanningsetatens administrasjon og de undersøkte skolene har

verifisert de delene av framstillingen som var relevante for dem, og hele rapporten har vært underlagt intern kvalitetssikring i Kommunerevisjonen.

Samlet sett mener vi at faktabeskrivelsen gir et tilfredsstillende gyldig og pålitelig grunnlag for våre vurderinger, konklusjoner og anbefalinger.

Vedlegg 3 Uttalelse fra Byrådsavdeling for oppvekst og kunnskap

Byrådsavdeling for oppvekst og kunnskap Oslo

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

Deres ref.:	Vår ref. (saksnr.):	Saksbeh.:	Dato:
21/1187 - 95	20/2791 - 10	Linda Elisabeth Heen, 908 51 118	13.01.2023

Svar på rapport til uttalelse - Personvern i skoler

Vi viser til brev med rapport til uttalelse, med følgende anbefalinger:

Kommunerevisjonen anbefaler at begge skolene iverksetter tiltak for å

- *sikre at den har oversikt over sin behandling av personopplysninger, og at den gjennomfører nødvendige risikovurderinger og personvernkonsekvensvurderinger, når dette ikke er gjort av Utdanningsetaten sentralt.*
- *sikre at tilgang til elevers personopplysninger er i tråd med tjenstlig behov.*
- *sikre at ansatte har tilfredsstillende kompetanse når det gjelder ivaretakelse av elevers personvern.*
- *sikre at personvernavvik blir tilfredsstillende håndtert, herunder fanget opp, lukket og fulgt opp.*

Utdanningsetaten sentralt utfører oppgaver knyttet til personvern og informasjonssikkerhet som ellers ville ha ligget til den enkelte skole. Etatens arbeid er en viktig del av rammene for skolenes arbeid på området. Kommunerevisjonen anbefaler at Utdanningsetaten:

- *legger til rette for at skolene kan behandle særlige kategorier personopplysninger og andre sensitive personopplysninger på en tilfredsstillende måte, herunder i*
- *samhandlingen mellom lærere og ledelse.*
- *viderefører arbeidet med å sikre at elevers personopplysninger ivaretas i Osloskolen.*
- *følger opp de undersøkte skolenes forbedringsarbeid knyttet til deres behandling av elevers personopplysninger.*

Kommunerevisjonen anbefaler at byråden for oppvekst og kunnskap følger opp Utdanningsetatens forbedringsarbeid knyttet til etatens behandling av elevers personopplysninger.

Her følger kommentarer fra Byråd for oppvekst og kunnskap:

1.Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?
Ja

2.Har byråden kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?

Oslo kommune
Byrådsavdeling for oppvekst og kunnskap

Besøksadresse:
Rådhuset
Postadresse:
Rådhuset, 0037 OSLO

Telefon: 21 80 21 80
postmottak@byr.oslo.kommune.no
Org. Nr.: 974767597
oslo.kommune.no

Byråden har ingen kommentar til metoden med tanke på rapportens konklusjoner. Revisjonen har undersøkt praksis ved to utvalgte skoler og noe om Utdanningsetatens sentrale arbeid knyttet til personvern og informasjonssikkerhet. Undersøkelsesperioden har vært skoleåret 2020/21 og 2021/22. Naturlig nok er det vanskelig å si noe om hvor representative funnene er for andre skoler i Oslo, men det ligger uansett viktige læringspunkter i rapporten. Utdanningsetaten har prioritert arbeid med informasjonssikkerhet og personvern høyt de siste årene og vi ser at det gir resultater. Det er derfor grunn til å tro at noe kan ha blitt forbedret siden undersøkelsesperioden.

3.Har byråden kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?
Nei

4.Hva er byrådens samlede vurdering av rapportens konklusjoner?
Håndtering av personopplysninger er en stor utfordring for skolene, på bakgrunn av at det brukes mange ulike løsninger for å løse lovpålagte oppgaver og gi tilpasset undervisning, det håndteres en stor mengde personopplysninger og det er mange brukere. Det stiller store krav til kompetanse i skolene, som kan være krevende å håndtere med den organisering man har i dag. Derfor er det etter vår vurdering hensiktsmessig at Utdanningsetaten i så stor grad som mulig legger til rette for at personvern blir godt håntert ute i skolene. Etaten har de siste årene økt ressursene og innsatsen for å styrke dette arbeidet. Rapporten peker på viktige forbedringspunkter i det videre arbeidet på området både sentralt i etaten og hva som blir viktig å følge opp overfor de enkelte skolene.

5.Vil byråden vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner? I tilfelle hvilke?
Byrådsavdeling for oppvekst og kunnskap har allerede en tett dialog med Utdanningsetaten for å følge opp arbeidet med personvern i skolesektoren, og vil som en del av denne dialogen følge opp arbeidet med konklusjonene fra rapporten. Personvern er tema i styringsdialogen gjennom etatsstyringsmøter samt gjennom rapportering av ledelsens gjennomgang og virksomhetsleders egenerklæring og eget møte i forbindelse med rapporteringen.

6.Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?
Byrådsavdelingens oppfølgning av Utdanningsetaten forbedringsarbeid er et kontinuerlig og langsiktig arbeid.

7.Oppfattes rapporten som nyttig for byråden? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.
Rapporten oppleves som nyttig, se svar ovenfor.

8.Hvordan vurderes rapportens oppbygning og språkbruk?
Rapporten har etter vår vurdering en god oppbygging og språkbruk.

Med vennlig hilsen

Hege Sevatdal
kommunaldirektør

Hege Sevatdal
kommunaldirektør

Vedlegg 4 Uttalelse fra Utdanningsetaten

Utdanningsetaten

Oslo

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

Unntatt offentlighet
Offl. § 5 andre ledd

Deres ref.:	Vår ref. (saksnr.):	Saksbeh.:	Dato:
21/1187	21/43813 - 12	Marie Innvær Hovland, 992 44 174	05.01.2023

Uttalelse vedrørende Kommunerevisjonens rapport "Personvern i skoler"

Utdanningsetaten viser til brev fra Kommunerevisjonen 9. desember 2022 om forvaltningsrevisjon knyttet til personvern i skoler.

I brevet ber Kommunerevisjonen om tilbakemelding på rapporten, og i tillegg om svar på åtte spørsmål.

Kommunerevisjonen ber om at Utdanningsetaten og de to utvalgte skolene avtaler om svar sendes individuelt eller samlet. I det videre følger Utdanningsetaten, Hauketo og Nordseter skolers svar samlet.

1. **Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?**

   Både Utdanningsetaten og de to skolene mener at informasjonen om prosjektets hensikt har vært tilstrekkelig klar.

2. **Har etaten kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?**

   Hverken Utdanningsetaten eller de to skolene har kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner.

3. **Har etaten kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?**

   Hverken Utdanningsetaten eller de to skolene har kommentarer til revisjonskriteriene.

4. **Hva er etatens samlede vurdering av rapportens konklusjoner?**

   Utdanningsetaten mener rapporten på en nyttig måte bidrar til å sette søkelyset på personvern i Osloskolen. Videre mener Utdanningsetaten at rapporten i stor grad samsvarer med det bildet etaten selv har av tilstanden på området, og de utfordringer vi kontinuerlig jobber med å løse på stadig bedre måte.

   De to skolene har ingen kommentarer på dette punktet.

5. **Vil etaten vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner? I tilfelle hvilke?**

Utdanningsetaten
Oslo kommune

Besøksadresse:
Grensesvingen 6, 0660 Oslo
Postadresse:
Postboks 6127 Etterstad
0602 Oslo

Telefon: 21 80 21 80
postmottak@osloskolen.no
Org. Nr.: 976820037

Utdanningsetaten vil, fortsette å jobbe for å bedre elevenes personvern i Osloskolen. Vi vil grundig gjennomgå Kommunerevisjonens anbefalinger i kapittel 7.2 og lage en prioritert oppfølgingsplan.

Hauketo og Nordseter skoler planlegger følgende tiltak:

- Opplæring av nyansatte fra og med høsten 2023
- Opplæring av alle ansatte. Dette er iverksatt og videreføres
- Skriftliggjøring av rutiner (januar-juni 2023)
- Rutiner for risikovurdering av innsamling og lagring av personverninformasjon (Kontinuerlig)
- Rutiner for avvikshåndtering informeres om og iverksettes. (Januar-mars 2023)

6. **Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?**

   Utdanningsetaten har som mål å starte opp de fleste tiltakene i løpet av 2023.

   Nordseter skole skriver at arbeidet begynner vår 2023, og skal være formalisert og gjort kjent for ansatte innen skolestart høsten 2023.

7. **Oppfattes rapporten som nyttig for etaten? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.**

   Utdanningsetaten oppfatter rapporten som nyttig for videre utviklingsarbeid. Rapporten oppfattes som en god kvalitetssikring av etatens pågående arbeid innen informasjonssikkerhet og personvern.

8. **Hvordan vurderes rapportens oppbygning og språkbruk?**

   Utdanningsetaten vurderer rapportens oppbygging og språkbruk som god.

Med vennlig hilsen

Anita Capjon Bergh
juridisk direktør

Marie Innvær Hovland
juridisk rådgiver

Dokumentet er elektronisk godkjent

Oslo

Oslo Kommune
Kommunerevisjonen
Fredrik Selmers vei 3
0663 Oslo

Tel. +21 80 21 80

Rapport 2/2023

Du finner mer informasjon om Kommunerevisjonen og våre rapporter på:
www.krv.oslo.kommune.no